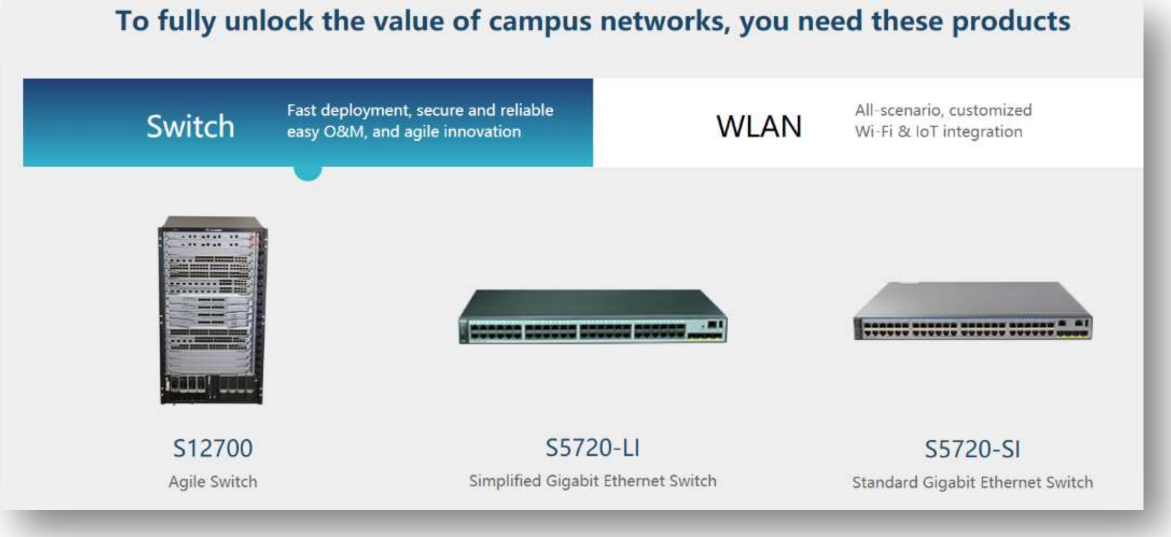
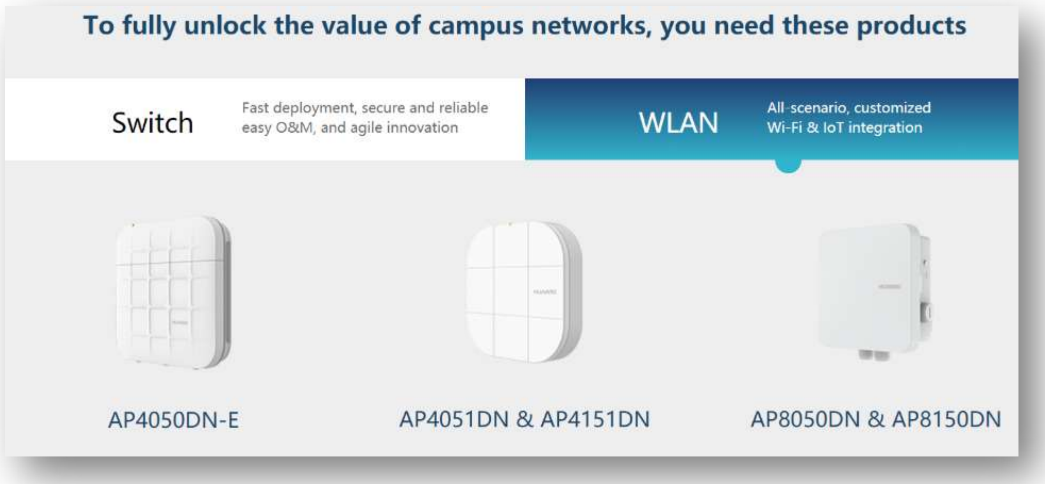
Harris Corporation v. Huawei, et al – Case No. 2:18-cv-439
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
AMENDED Exhibit F – U.S. Patent No. 7,327,690 ('690) – Claims 32-34, 36, 38-43, 71-73, 75-80

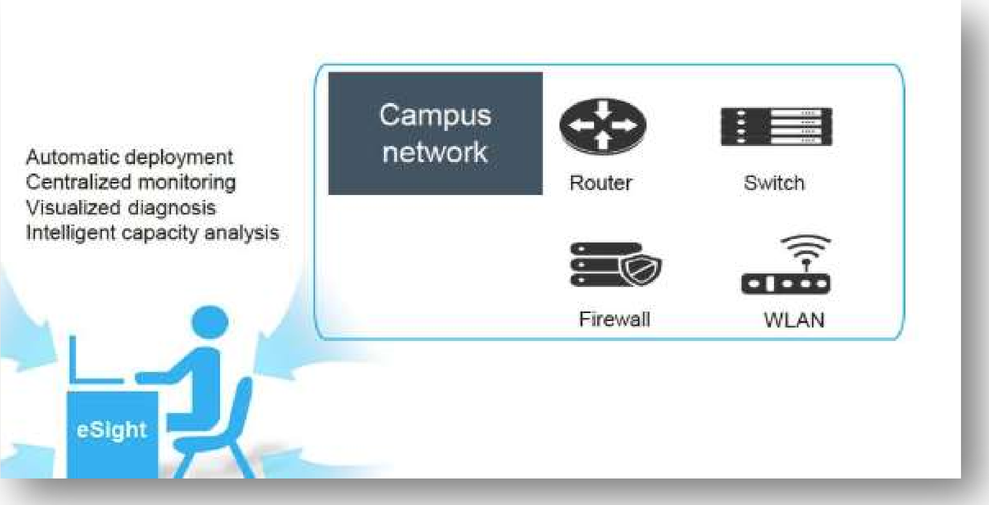
Harris Corporation expressly reserves the right to supplement or modify these Disclosures as appropriate upon receipt of further information and discovery. The Huawei '690 Patent Accused Products (as that term is defined and the corresponding devices are identified in Harris's P.R. 3-1 and P.R. 3-2 disclosures cover pleading) infringe at least the following claims. References to instrumentalities in this chart are exemplary only and should not be construed as limiting the scope of any claim of the '690 patent. The Huawei '690 Patent Accused Products satisfy each claim element below literally. The Huawei '690 Patent Accused Products also satisfy claim elements under the Doctrine of Equivalents, including without limitation where specifically identified below, because they include and perform substantially similar functionality.

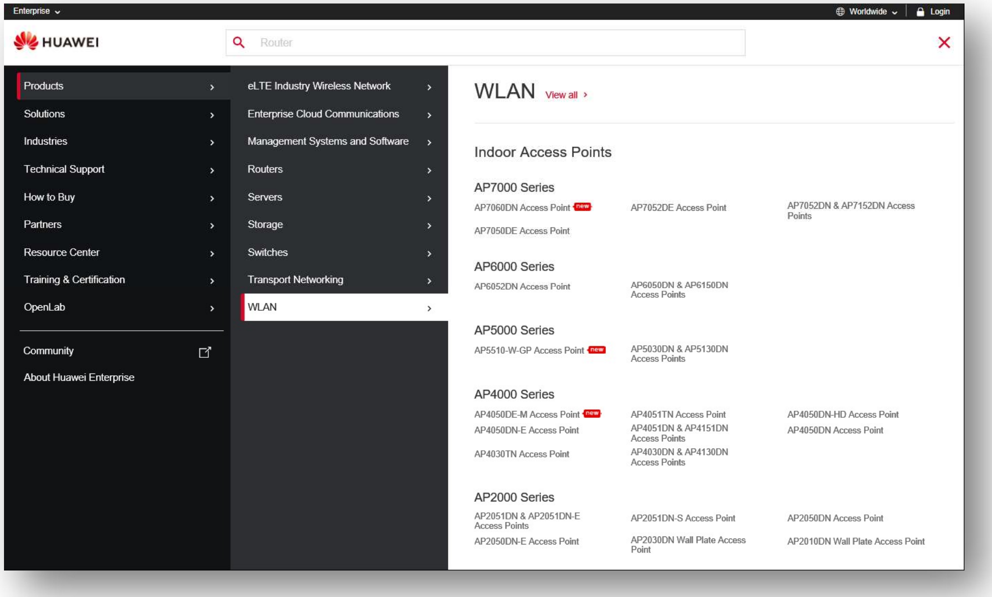
'690 Patent Claim 32	**Infringement By Huawei Corporation**
32. A wireless local or metropolitan area network comprising:	The Huawei '690 Patent Accused Products infringe this claim. Huawei makes, uses, sells, offers to sell and/or imports equipment used in wireless local or metropolitan area networks, including its WLAN products and consumer devices, and on information and belief, makes, uses, sells, offers to sell and/or imports wireless local or metropolitan area networks in the United States. Without the benefit of discovery, Harris identifies exemplary networks, including, without limitation, networks deployed at Huawei's 13 U.S. facilities; networks deployed in CloudCampus solutions such as those deployed for Cloud4Wi, in San Francisco, CA; other enterprise networks deployed for Weichai Power in Chicago, Ill., and Crowley Independent School District in Crowley, Tx. On information and belief, Huawei's United States Offices utilize the Huawei WLAN products to form a wireless local or metropolitan area network (Wireless LAN/MAN). These offices include Huawei Technologies USA, Inc. HQ's offices in Plano, Texas; Broomfield, CO; Houston, TX, Reston, VA; Philadelphia, PA; Irvine, CA; Cupertino, CA; Huawei Device USA, Inc. HQ's offices in Plano, Tx; Bellevue, WA; Mountain View, CA; Alpharetta, GA; Bridgewater, NJ; Santa Clara, CA; and San Diego, CA, as well as Futurewei Technologies, Inc.'s offices in Santa Clara, CA; Plano, TX, Bridgewater, NJ; Rolling Meadows, IL; Greensboro, NC; Louisville, CO; San Diego, CA; and Bellevue, WA. https://www.huawei.com/us/contact-us#office

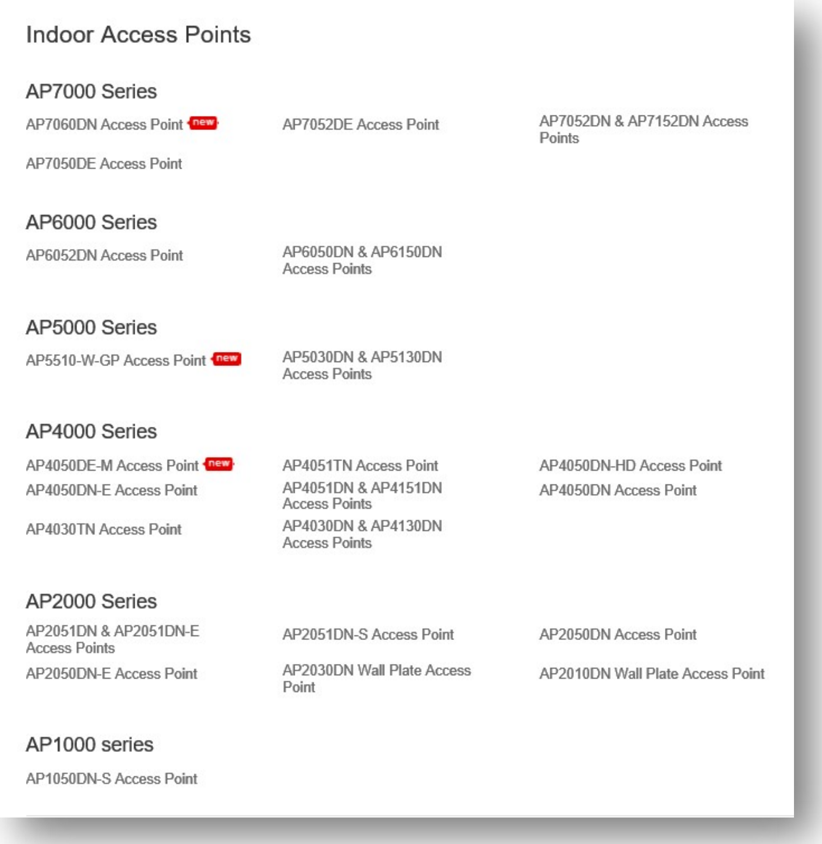
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Further, in 2017, Huawei partnered with Cloud4Wi in San Francisco California to install its CloudCampus solution. *See* https://cloud4wi.com/cloud4wi-and-huawei/ Huawei CloudCampus solutions utilize various switches and access points, for example:  To fully unlock the value of campus networks, you need these products Switch — Fast deployment, secure and reliable easy O&M, and agile innovation WLAN — All-scenario, customized Wi-Fi & IoT integration S12700 Agile Switch S5720-LI Simplified Gigabit Ethernet Switch S5720-SI Standard Gigabit Ethernet Switch

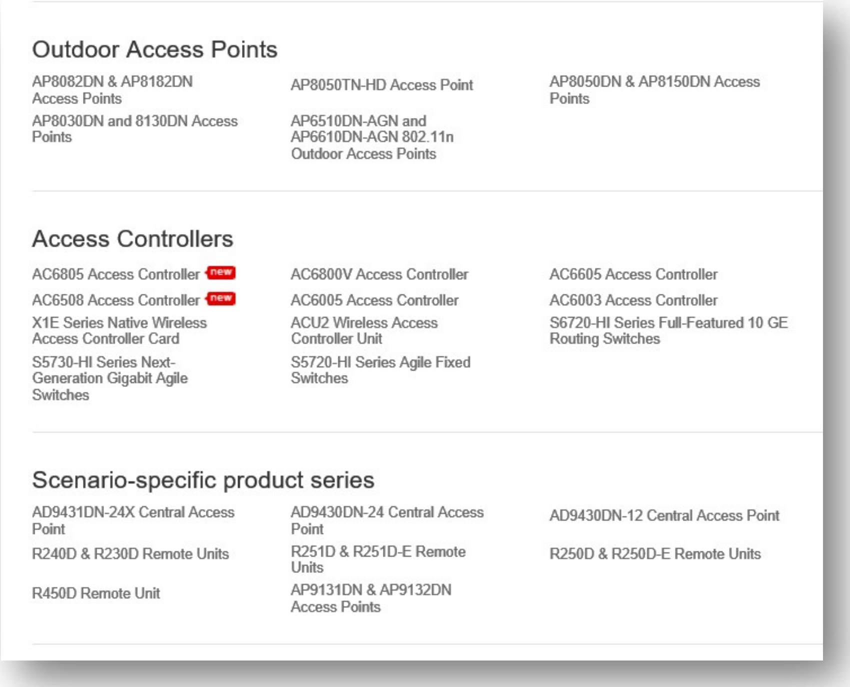
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 To fully unlock the value of campus networks, you need these products Switch Fast deployment, secure and reliable easy O&M, and agile innovation WLAN All-scenario, customized Wi-Fi & IoT integration AP4050DN-E AP4051DN & AP4151DN AP8050DN & AP8150DN http://e.huawei.com/topic/cloudcampus-en/index.html

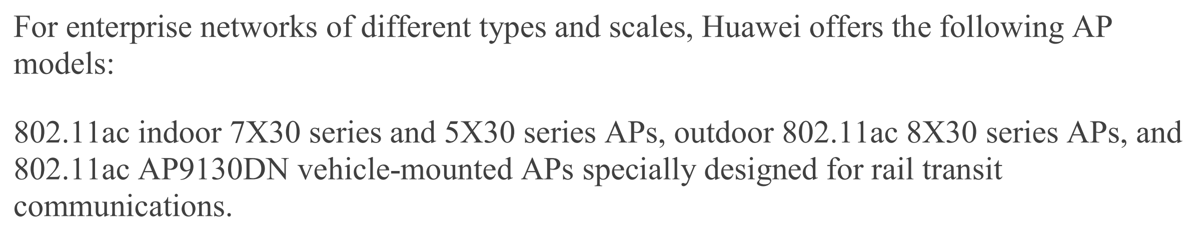
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 CloudCampus Products and S Controller and analyzer Agile CONTROLLER Campus Insight Cloud managed modular switches S12704 S12708 S12712 Flexible 8-48 port combinations, 88 switch models Automatic 2.5G/5G/10G adaptation S6720-32C-PWH-SI S5320/S5720 S6320/S6720 10GE switch All series 23 indoor and outdoor AP models 802.11ax AP AP7060DN Dual 5G Outdoor AP8082DN Indoor AP Outdoor AP Agile distributed AP https://e.huawei.com/en/material/onLineView?MaterialID=0b6395888b2a4bd49613a9bc28f3e95c at 15.

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Further, Campus networks are an exemplary network that may work with Huawei eSight:  Automatic deployment Centralized monitoring Visualized diagnosis Intelligent capacity analysis Campus network Router Switch Firewall WLAN eSight eSight Overview Presentation at 6. On information and belief, all Huawei WLAN products incorporate the Wireless Intrusion Detection System (WIDS) as described, for example in the WIDS and WIPS Technology White Paper: "The Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions monitor and prevent the preceding attacks on WLANs. This document describes WIDS and WIPS technologies used by Huawei WLAN products." Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 1.

'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	Huawei website currently lists the following WLAN products:  Enterprise Worldwide Login HUAWEI Router Products Solutions Industries Technical Support How to Buy Partners Resource Center Training & Certification OpenLab Community About Huawei Enterprise eLTE Industry Wireless Network Enterprise Cloud Communications Management Systems and Software Routers Servers Storage Switches Transport Networking WLAN View all WLAN Indoor Access Points AP7000 Series AP7060DN Access Point new AP7052DE Access Point AP7052DN & AP7152DN Access Points AP7050DE Access Point AP6000 Series AP6052DN Access Point AP6050DN & AP6150DN Access Points AP5000 Series AP5510-W-GP Access Point new AP5030DN & AP5130DN Access Points AP4000 Series AP4050DE-M Access Point new AP4051TN Access Point AP4050DN-HD Access Point AP4050DN-E Access Point AP4051DN & AP4151DN Access Points AP4050DN Access Point AP4030TN Access Point AP4030DN & AP4130DN Access Points AP2000 Series AP2051DN & AP2051DN-E Access Points AP2051DN-S Access Point AP2050DN Access Point AP2050DN-E Access Point AP2030DN Wall Plate Access Point AP2010DN Wall Plate Access Point

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Indoor Access Points AP7000 Series AP7060DN Access Point new · AP7052DE Access Point · AP7052DN & AP7152DN Access Points AP7050DE Access Point AP6000 Series AP6052DN Access Point · AP6050DN & AP6150DN Access Points AP5000 Series AP5510-W-GP Access Point new · AP5030DN & AP5130DN Access Points AP4000 Series AP4050DE-M Access Point new · AP4051TN Access Point · AP4050DN-HD Access Point AP4050DN-E Access Point · AP4051DN & AP4151DN Access Points · AP4050DN Access Point AP4030TN Access Point · AP4030DN & AP4130DN Access Points AP2000 Series AP2051DN & AP2051DN-E Access Points · AP2051DN-S Access Point · AP2050DN Access Point AP2050DN-E Access Point · AP2030DN Wall Plate Access Point · AP2010DN Wall Plate Access Point AP1000 series AP1050DN-S Access Point

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Outdoor Access Points AP8082DN & AP8182DN Access Points AP8050TN-HD Access Point AP8050DN & AP8150DN Access Points AP8030DN and 8130DN Access Points AP6510DN-AGN and AP6610DN-AGN 802.11n Outdoor Access Points Access Controllers AC6805 Access Controller new AC6800V Access Controller AC6605 Access Controller AC6508 Access Controller new AC6005 Access Controller AC6003 Access Controller X1E Series Native Wireless Access Controller Card ACU2 Wireless Access Controller Unit S6720-HI Series Full-Featured 10 GE Routing Switches S5730-HI Series Next-Generation Gigabit Agile Switches S5720-HI Series Agile Fixed Switches Scenario-specific product series AD9431DN-24X Central Access Point AD9430DN-24 Central Access Point AD9430DN-12 Central Access Point R240D & R230D Remote Units R251D & R251D-E Remote Units R250D & R250D-E Remote Units R450D Remote Unit AP9131DN & AP9132DN Access Points https://e.huawei.com/us/products/enterprise-networking/wlan (as of March 13, 2019). *See also, e.g.,* Huawei Access Point Datasheets ("*Rogue device monitoring Huawei APs support WIDS/WIPS, and can monitor, identify, defend, counter, and perform refined management on the rogue devices, to provide security guarantees for air interface environment and wireless data transmission.*") On information and belief, all APs support WIDS, *see also, e.g.,* AP2030DN at 2; AP4050DN-E at 3; AP4051DN & AP4151DN at 3; AP8050DN & AP8150DN at 3; AP6052DN at 4; AP6050DN&AP6150DN at 4. *See also* AP3050DE Product Description, *available at*

’690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	https://support.huawei.com/enterprise/en/wlan/ap3050de-pid-23482930?offeringId=21946538, at 13 (“Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist”); Huawei AP7060DN Access Point Data Sheet, *available at* https://e.huawei.com/en/related-page/products/enterprise-network/wlan/indoor-access-points/ap7060dn/wlan-ap7060dn, at 3 (“Huawei APs support WIDS/WIPS, . . .”). *See also,* Huawei Enterprise AP Series 802.11ac Brochure:  For enterprise networks of different types and scales, Huawei offers the following AP models: 802.11ac indoor 7X30 series and 5X30 series APs, outdoor 802.11ac 8X30 series APs, and 802.11ac AP9130DN vehicle-mounted APs specially designed for rail transit communications.

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION

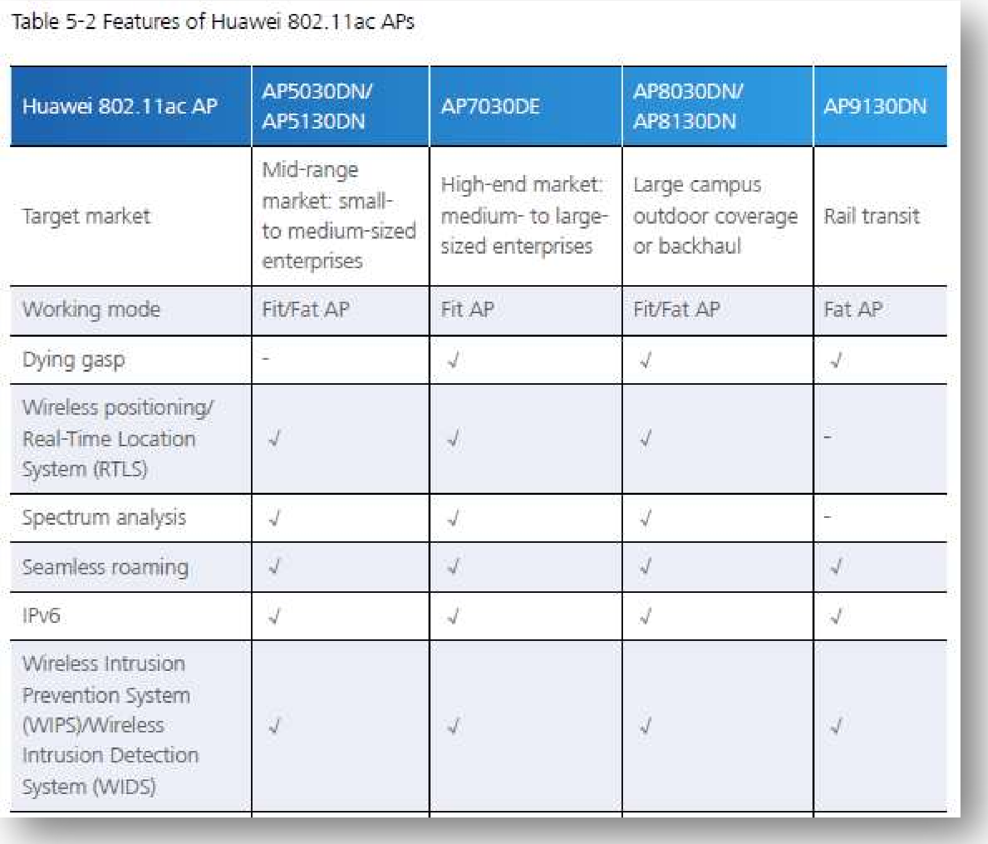


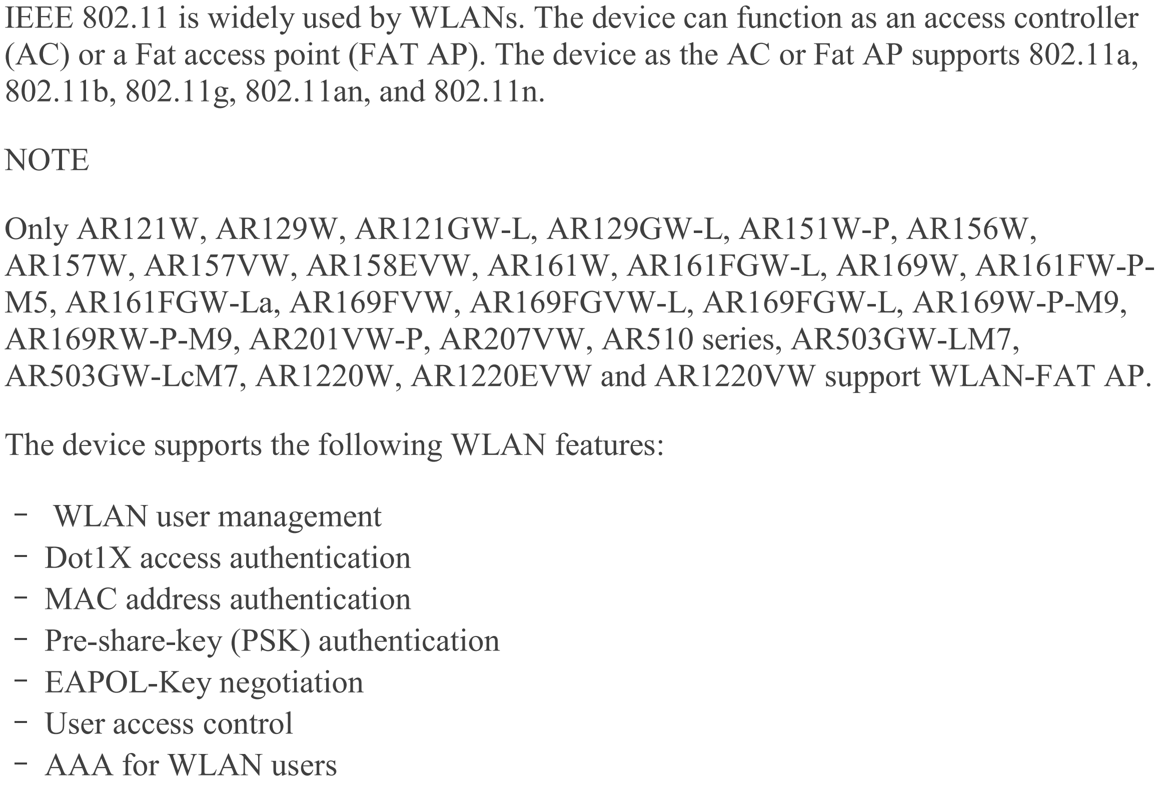
Table 5-2 Features of Huawei 802.11ac APs

Huawei 802.11ac AP	AP5030DN/ AP5130DN	AP7030DE	AP8030DN/ AP8130DN	AP9130DN
Target market	Mid-range market: small- to medium-sized enterprises	High-end market: medium- to large-sized enterprises	Large campus outdoor coverage or backhaul	Rail transit
Working mode	Fit/Fat AP	Fit AP	Fit/Fat AP	Fat AP
Dying gasp	-	√	√	√
Wireless positioning/ Real-Time Location System (RTLS)	√	√	√	-
Spectrum analysis	√	√	√	-
Seamless roaming	√	√	√	√
IPv6	√	√	√	√
Wireless Intrusion Prevention System (WIPS)/Wireless Intrusion Detection System (WIDS)	√	√	√	√

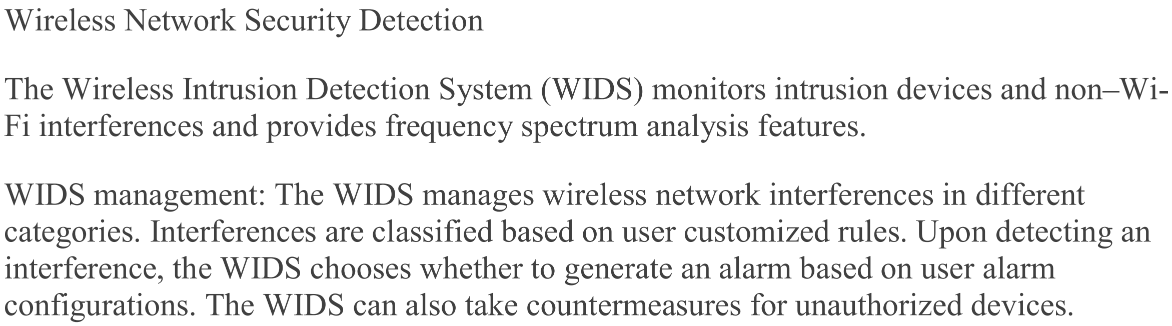
Huawei Routers deployed in a WLAN have various other security mechanisms, including:

"3.2.4 Security

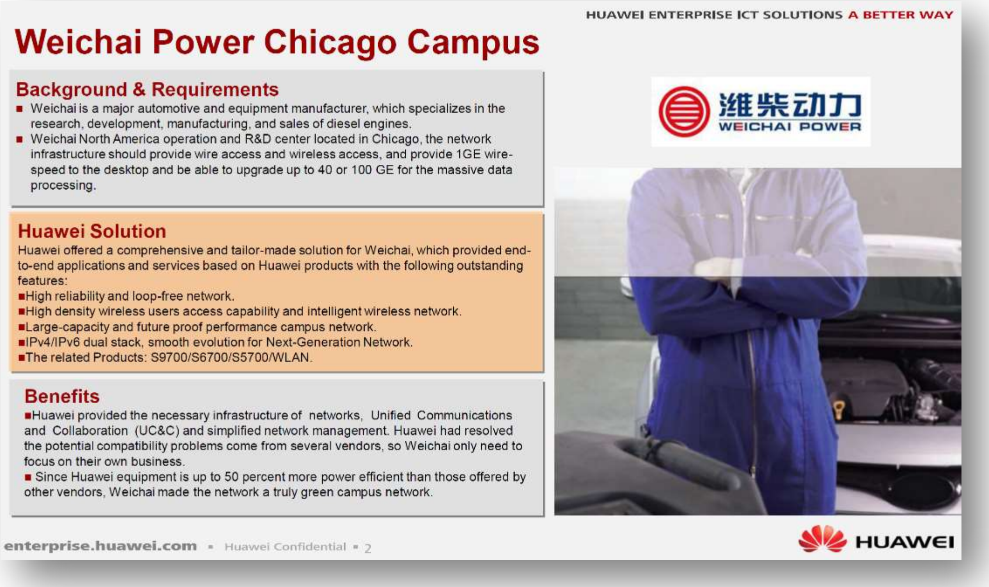
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	… NAC Network Admission Control (NAC) is an end-to-end access security framework and includes… MAC address authentication" Huawei AR120&AR150&AR160&AR200&AR500&AR510&AR1 200&AR2200&AR3200&AR3600 Series Enterprise Routers Product Description, Issue 05 (2016-06-15) at 43. Routers may further operate as an Access Controller and provides MAC address authentication for WLAN: "3.2.6 WLAN A wireless local area network (WLAN) connects two or more computers or devices and enables the devices to communicate by using the wireless telecommunication technology. WLAN uses the wireless technology to implement fast Ethernet access. The primary advantage of WLAN is that terminals, such as computers, can access a network through a wireless medium rather than a physical cable. This facilitates network construction and allows users to move around without interrupting communication. WLAN is more flexible than traditional wired access. WLAN is widely used in public areas such as on campuses, business centers, and airports. The WLAN uses cables at the backbone layer, and users access the WLAN through one or more access points (APs) using radio waves. The transmission distance of an AP is tens of meters.

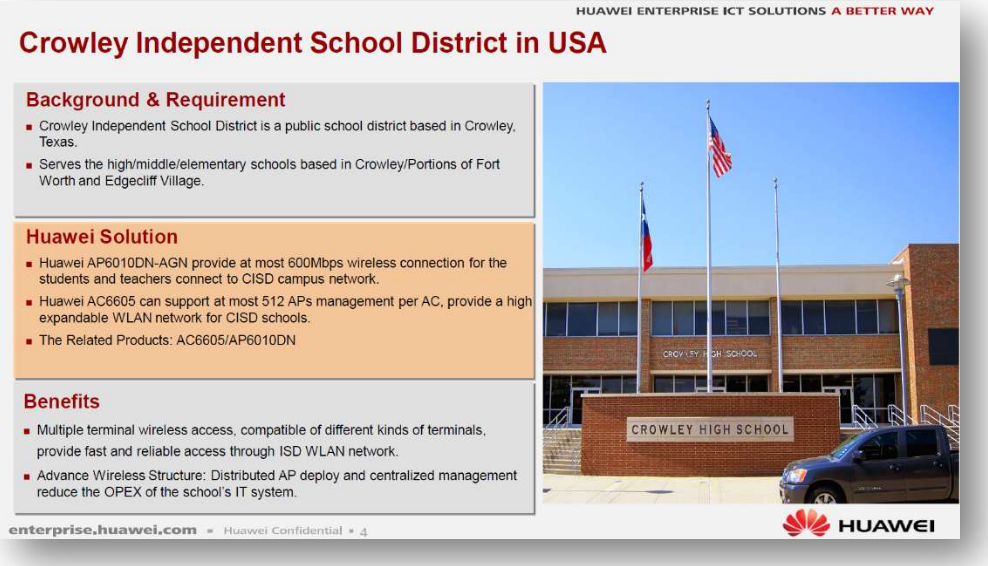
'690 Patent Claim 32	Infringement By Huawei Corporation
	 IEEE 802.11 is widely used by WLANs. The device can function as an access controller (AC) or a Fat access point (FAT AP). The device as the AC or Fat AP supports 802.11a, 802.11b, 802.11g, 802.11an, and 802.11n. NOTE Only AR121W, AR129W, AR121GW-L, AR129GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161FGW-L, AR169W, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR510 series, AR503GW-LM7, AR503GW-LcM7, AR1220W, AR1220EVW and AR1220VW support WLAN-FAT AP. The device supports the following WLAN features: – WLAN user management – Dot1X access authentication – MAC address authentication – Pre-share-key (PSK) authentication – EAPOL-Key negotiation – User access control – AAA for WLAN users Huawei AR120&AR150&AR160&AR200&AR500&AR510&AR1 200&AR2200&AR3200&AR3600 Series Enterprise Routers Product Description, Issue 05 (2016-06-15) at 47. *See also, e.g.,* Huawei Remote Unit Datasheets: R450D at 6 ("*Security features - WIDS including rogue AP and STA detection, attack detection, STA/AP blacklist and whitelist… -Intrusion prevention*"); R251D & R251D-E ("*Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist*").

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	See also, e.g., Huawei Access Points (FATAP), V200R007C20, MIB Reference, Issue 05 (2019-03-15), *available at* https://support.huawei.com/enterprise/en/doc/EDOC1000154350, at Table 1 (listing products), 145-146, 1447-1515 and 2638-2712 (WIDS), 2790-2848 ("Station" / "STA" tables). Huawei consumer devices, including laptops, phones and tablets, are also designed to communicate with wireless networks via the IEEE 802.11 protocols. For example, specifications for Huawei smartphones such as the Huawei Mate SE indicate that they support "802.11b/g/n, 2.4 GHz" connectivity and the "Android N+EMUI 5.1" operating system. https://consumer.huawei.com/us/phones/mate-se/specs/. Specifications for Huawei's Mate 10 Pro smartphones indicate that they support "Wi-Fi 2.4G/5G, 802.11a/b/g/n/ac with Wi-Fi Direct support" connectivity and the "Android 8.0" and "EMUI 8.0" operating system. https://consumer.huawei.com/us/phones/mate10-pro/specs/. Specifications for Huawei laptops and tablets such as the Matebook 13 indicate that they support "IEEE 802.11a/b/g/n/ac" connectivity. https://consumer.huawei.com/en/laptops/matebook-13/specs/. Huawei consumer devices, including laptops, phones and tablets, also participate in the WIDS system as client stations (also referred to in WIDS and documentation as "STAs" or "ad hoc" devices). *See, e.g.*, Huawei Technologies Co., Ltd., *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 7 ("When receiving a Probe Request, an Association Request, or a Reassociation Request frame, the AP determines whether the sender is an ad hoc device or STA based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame") *see also id.* at 11 ("Rogue STAs: After detecting a rogue STA, a monitor AP uses the BSSID and MAC address of the rogue STA to send a fake unicast Deauthentication frame to contain it. A STA whitelist can also be configured to prevent STAs in the STA whitelist from associating with rogue APs"). *See also* Huawei Access Points (FATAP), V200R007C20, MIB Reference, Issue 05 (2019-03-15), at 145-146 (MAC authentication table), 1447-1515 and 2638-2712 (WIDS), 2790-2848 ("Station" / "STA" tables). Accordingly, and as further detailed herein, these devices implement aspects of the WIDS system within the "wireless local or metropolitan area network" of the claim (also referred to as a Wireless LAN/MAN in the patent specification).

'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	On information and belief Huawei consumer devices, including laptops, phones and tablets also can participate in the WIDS system as access points ("APs"), including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also implement intrusion detection according to the claim. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security."). The Huawei eSight and eSight Network further incorporates the WIDS system:  Wireless Network Security Detection The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non–Wi-Fi interferences and provides frequency spectrum analysis features. WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices. Huawei eSight Full Product Datasheet, CH 12 eSight WLAN Manager; p. 53 (2013-09-03) Huawei Technologies Co., Ltd.; *see also* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 58-59 (indicating that, on information and belief, all versions of eSight incorporate WIDS).

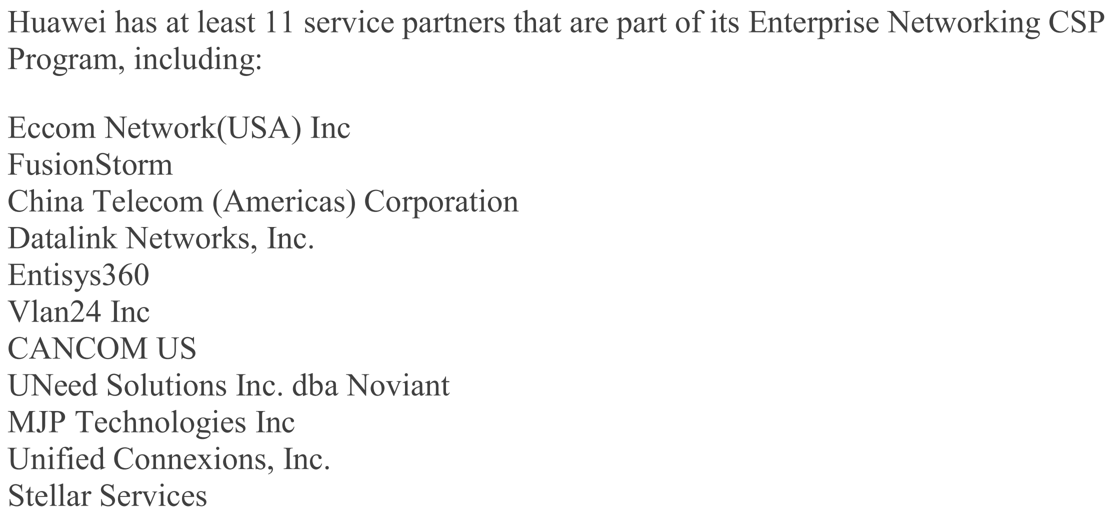
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	In another non-limiting example, Huawei installed a Wireless local or metropolitan area network at Waichai in Chicago, Illinois using S9700/S6700/S5700/WLAN products: The [Weichai North America] center located in suburban Chicago, which covers 20-acre parcel, and over 300 engineers will be working in this center. … Huawei offered a comprehensive and tailor-made solution for Weichai, which provided end-to-end applications and services based on Huawei products [including] Two clustered S9706 LAN switches stacking with service interfaces at core layer combined with stacked gigabyte access S5700 POE LAN switches to create a loop-free network with high reliability. • High density wireless users access capability and intelligent wireless network The Huawei AP6010 LAN access points provide integrated built-in MIMO antenna and spectrum analysis for even frequency coverage with no coverage hole, concurrent user access rate 20 percents higher than industry average. Moreover, wireless authentication and authorization can provide fine-grained access control for the security of WLAN network. … Huawei was chosen as the only vendor by Weichai… …

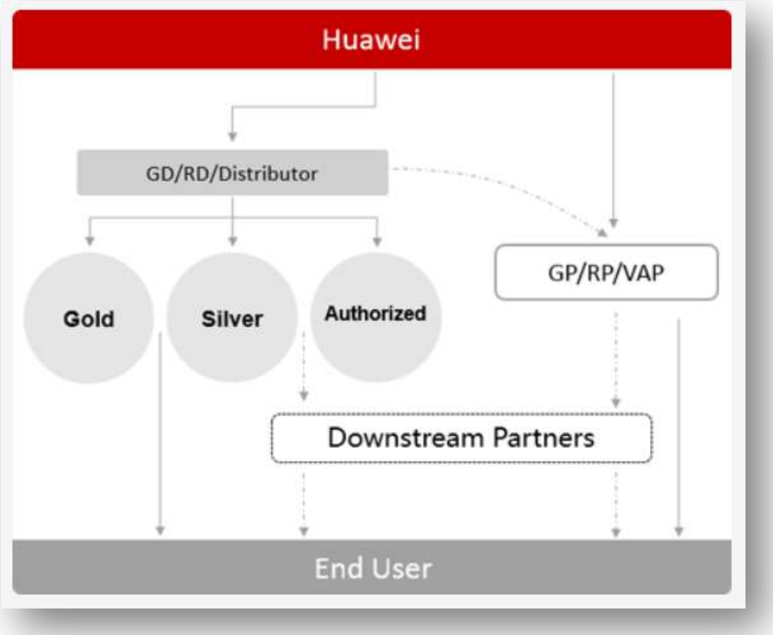
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Huawei provided the necessary infrastructure of networks, Unified Communications and Collaboration (UC&C), IT solutions and simplified network management. Huawei In Large Enterprise Case Studies at 12-13 (available at  HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY **Weichai Power Chicago Campus** **Background & Requirements** ■ Weichai is a major automotive and equipment manufacturer, which specializes in the research, development, manufacturing, and sales of diesel engines. ■ Weichai North America operation and R&D center located in Chicago, the network infrastructure should provide wire access and wireless access, and provide 1GE wire-speed to the desktop and be able to upgrade up to 40 or 100 GE for the massive data processing. **Huawei Solution** Huawei offered a comprehensive and tailor-made solution for Weichai, which provided end-to-end applications and services based on Huawei products with the following outstanding features: ■High reliability and loop-free network. ■High density wireless users access capability and intelligent wireless network. ■Large-capacity and future proof performance campus network. ■IPv4/IPv6 dual stack, smooth evolution for Next-Generation Network. ■The related Products: S9700/S6700/S5700/WLAN. **Benefits** ■Huawei provided the necessary infrastructure of networks, Unified Communications and Collaboration (UC&C) and simplified network management. Huawei had resolved the potential compatibility problems come from several vendors, so Weichai only need to focus on their own business. ■ Since Huawei equipment is up to 50 percent more power efficient than those offered by other vendors, Weichai made the network a truly green campus network. 潍柴动力 WEICHAI POWER enterprise.huawei.com ▪ Huawei Confidential ▪ 2 HUAWEI http://www.enterprisesolutions.altech.co.za/sites/.collab_d7_live/files/Huawei_in_Large_Enterprise%28include%20Small%20Campus%29_1.pdf) HUAWEI WLAN Successful Stories PowerPoint at 2. Huawei further installed networks at Crowley Independent Schools in Texas:

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY **Crowley Independent School District in USA** **Background & Requirement** ▪ Crowley Independent School District is a public school district based in Crowley, Texas. ▪ Serves the high/middle/elementary schools based in Crowley/Portions of Fort Worth and Edgecliff Village. **Huawei Solution** ▪ Huawei AP6010DN-AGN provide at most 600Mbps wireless connection for the students and teachers connect to CISD campus network. ▪ Huawei AC6605 can support at most 512 APs management per AC, provide a high expandable WLAN network for CISD schools. ▪ The Related Products: AC6605/AP6010DN **Benefits** ▪ Multiple terminal wireless access, compatible of different kinds of terminals, provide fast and reliable access through ISD WLAN network. ▪ Advance Wireless Structure: Distributed AP deploy and centralized management reduce the OPEX of the school's IT system. enterprise.huawei.com ▪ Huawei Confidential ▪ 4 HUAWEI HUAWEI WLAN Successful Stories PowerPoint at 4; *see also* http://support.huawei.com/en/about/media_center/video_clips_list/hw-341648.htm On information and belief, and as further discovery will show, Huawei has installed networks in other US locations, for example: > Sears, one of the leading US retail enterprises, decided to use Huawei's technology and equipment when upgrading the networks of hundreds of stores. Northern Michigan University, Crowley Independent School District in Texas and Digital Domain, a visual

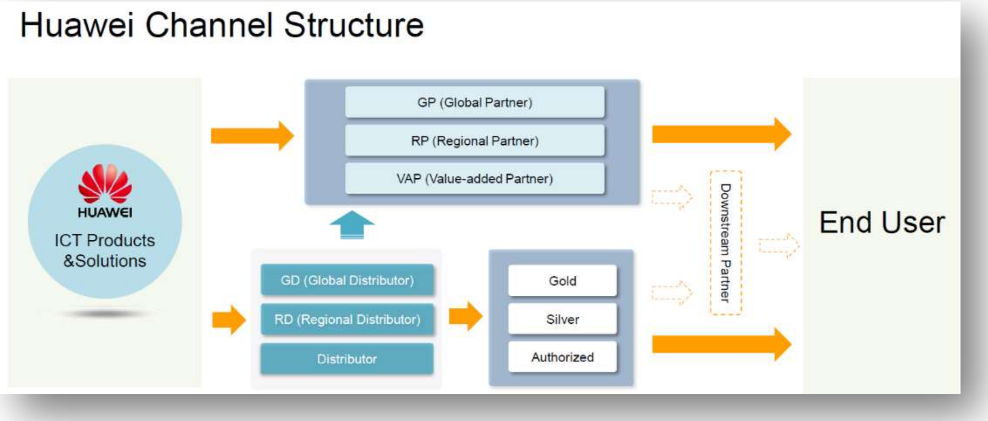
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	effects and digital production company in Hollywood, have adopted storage, Internet solutions and other services provided by Huawei. http://www.globaltimes.cn/content/864994.shtml On information and belief, all Huawei WLAN products, when combined to form a wireless local or metropolitan area network, are able to utilize the WIDS/WIPS technology. Huawei WLAN products are specifically designed to be linked together to form a wireless network, and to be used with other laptops, tablets, phones and WiFi capable devices, and Huawei directs and encourages such conduct. Accordingly, Huawei indirectly infringes this claim by inducing infringement. *See e.g.,* WLAN Installation Service, available at http://support.huawei.com/enterprise/NewsReadAction.action?newType=05&contentId=NEWS1000006056; Enterprise NMS and Application Software Installation Service, available at http://support.huawei.com/enterprise/NewsReadAction.action?newType=05&contentId=NEWS1000006040 and other channel partner service descriptions at https://e.huawei.com/en/partner/partner-program/services In yet a further example, Huawei has a 3, 4 and 5 Star and Global Certified Service Partner Certification program, in which, among other things, allows partners to receive Partner Enablement Support from Huawei. Service partners must meet certain requirements, for example:

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Certification Requirement • HCNA x 2 • **Domain:** Enterprise Networking (R&S, WLAN, and Security), or Enterprise Networking (Transmission and Access), or Enterprise Cloud Communications (UC, CC, VC, and IVS), or IT (Storage, Server, Cloud Computing, and DC), or Network Energy (DCF and UPS) https://e.huawei.com/en/partner/partner-program/Overview/Standard

'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	Huawei offers its partners numerous trainings and certificates related to Enterprise Network, including courses that train individuals on designing and deploying WLAN networks, including aspects of WIDS/WIPS and network security. *See, e.g.,* Training Description for Enterprise Network, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/channel%20partner%20program/legal%20-%20commercial/services/learning%20services/hw_201676; *see also* https://e.huawei.com/en/partner/partner-program/apply-for-specialization/network; see also https://e.huawei.com/en/partner/partner-program/Overview/Enablement ("Huawei's Training System Huawei offers a broad variety of training courses such as HALP training, e-learning, and instructor-led courses to help channel partners improve their capabilities.")  Huawei has at least 11 service partners that are part of its Enterprise Networking CSP Program, including: Eccom Network(USA) Inc FusionStorm China Telecom (Americas) Corporation Datalink Networks, Inc. Entisys360 Vlan24 Inc CANCOM US UNeed Solutions Inc. dba Noviant MJP Technologies Inc Unified Connexions, Inc. Stellar Services *See* https://e.huawei.com/en/partner/find-a-partner Huawei encourages its partners to "promote Huawei's brand in the enterprise business market.":

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Huawei GD/RD/Distributor Gold Silver Authorized GP/RP/VAP Downstream Partners End User Huawei's Channel Policy Principles The principle of Huawei's channel policy is "to work and collaborate on a win-win basis." Work and collaborate: Maximize the value for our channel partners and customers by motivating channel partners to explore the market and promote Huawei's brand in the enterprise business market.

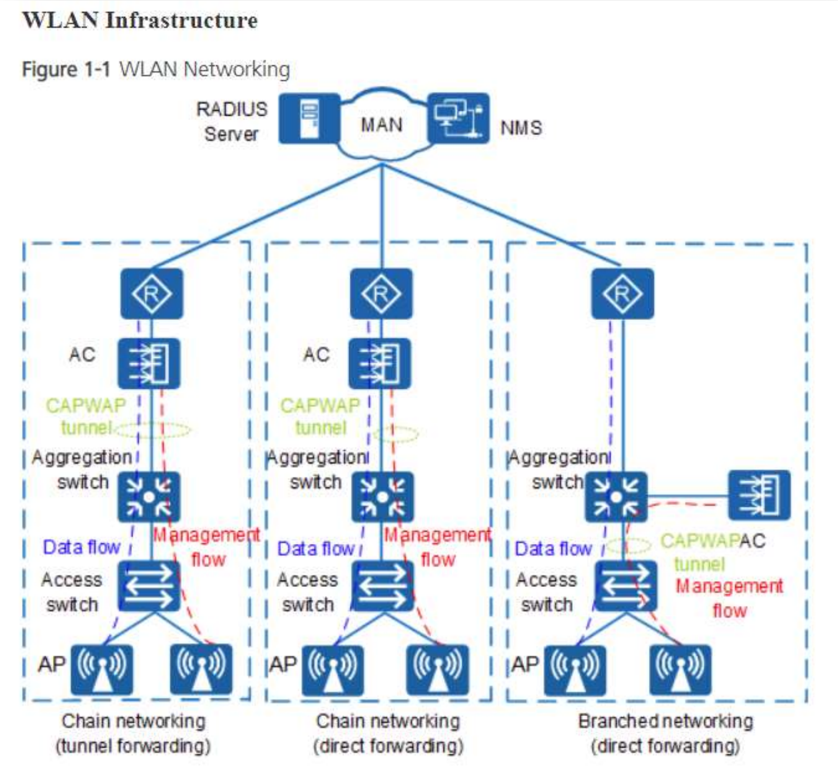
'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	Classification of Channel Partners Tier1 Partner: Distributor and Value Added Partner (VAP). Distributors include Global Distributors (GDs), Regional Distributors (RDs), and Local Distributors. Global Distributors and Regional Distributors are distributors that run business in multiple countries. Global Partners (GPs) and Regional Partners (RPs) work with Huawei in multiple countries and regions. Tier 2 Partner: Gold Partner, Silver Partner, and Authorized Partner For more information visit our Channel Partner Program page. https://e.huawei.com/en/partner/become-a-partner

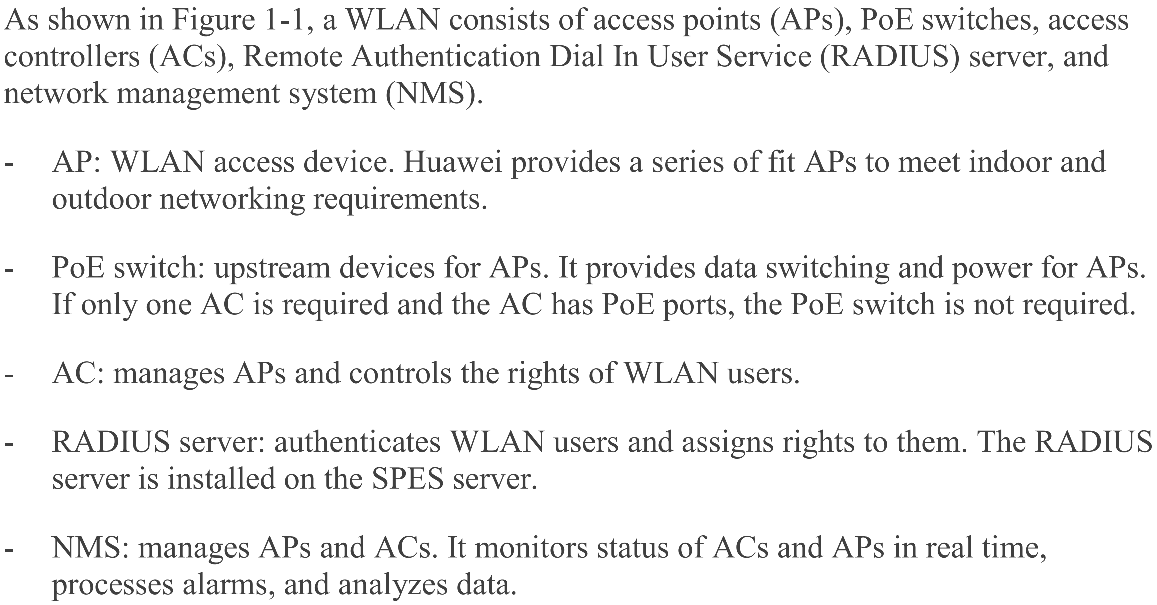
'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	 Huawei Channel Structure HUAWEI ICT Products &Solutions GP (Global Partner) RP (Regional Partner) VAP (Value-added Partner) GD (Global Distributor) RD (Regional Distributor) Distributor Gold Silver Authorized Downstream Partner End User Distributors must have "3 dedicated employees for Huawei enterprise business" and 6M sales performance thresholds Channel Partner Program Briefing 2018, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204 Further Distributors - Act as major partners of Huawei's Enterprise Business Group (BG) in regional markets. - Promise to accomplish business targets for related products and targets for distribution business. https://e.huawei.com/en/partner/partner-program/policy At least two Huawei Distributors exist in the United States,

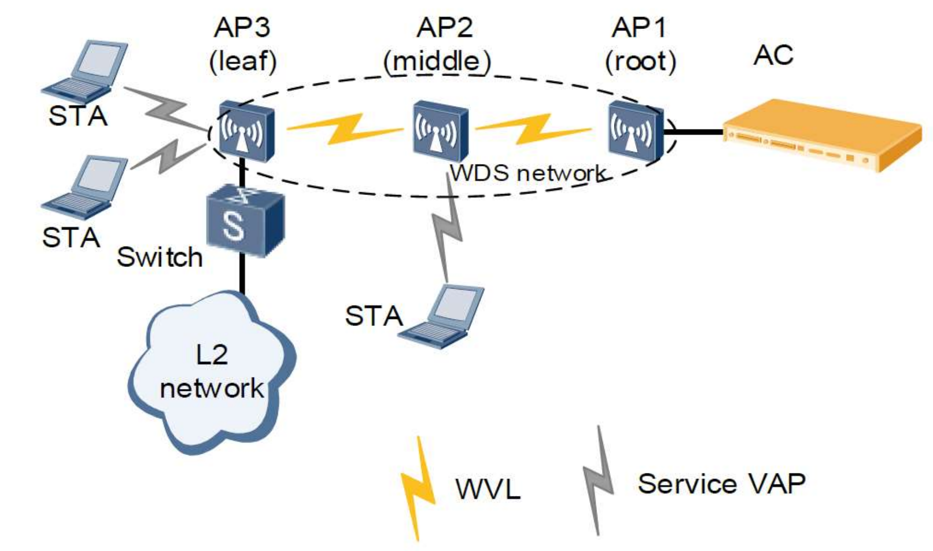
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	ASI Computer Technologies, Inc. in Fremont, CA; (selling Enterprise Cloud Communications, Data Center Switch, IT, Cloud Computing, Transport Network, Security, Access Network, Video Surveillance, Enterprise Networking Common, Campus Switch & WLAN, Enterprise Gateway, Router, UPS, Network Management) Wav, Inc. in Aurora Ill, (selling Data Center Switch, Enterprise Gateway, IT, Cloud Computing, Access Network, Network Management, Video Surveillance, Router, Enterprise Networking Common, Enterprise Cloud Communications, UPS, Campus Switch & WLAN, Transport Network, Security) https://e.huawei.com/en/partner/find-a-partner Value Added Partners must have a 2M sales performance threshold Channel Partner Program Briefing 2018, at p. 6, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204 Value Added Partners: - Act as major partners of Huawei's Enterprise BG in regional markets. - Promise to attain business targets for related industries and customers of Huawei's Enterprise BG. - Develop industry customer relationship platforms and provide support for Huawei's products to industry users. https://e.huawei.com/en/partner/partner-program/policy Value Added Partners in the United States that offer Enterprise Network products include:

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Proyectos Integrales Solares SL dba Proinso US LLC FusionStorm Consolidated Electrical Distri Rahi Systems, Inc Onesource Distributors, LLC Sonepar Management Us, Inc. CANCOM US WORLD WIDE TECHNOLOGY, LLC Wesco Distribution, Inc. Entisys360 China Telecom (Americas) Corporation *See* https://e.huawei.com/en/partner/find-a-partner Gold Partners in the United States that offer Enterprise Network products include Cloud Trekkers Technologies Inc Silver Partners in the United States that offer Enterprise Network products include Twotrees Technologies, LLC Mark III Systems, Inc UNeed Solutions Inc. dba Noviant Gold and Silver Partners have sales performance thresholds of 0.5M and 0.25M (Channel Partner Program Briefing 2018, at p. 6, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204 Gold and Silver Partners

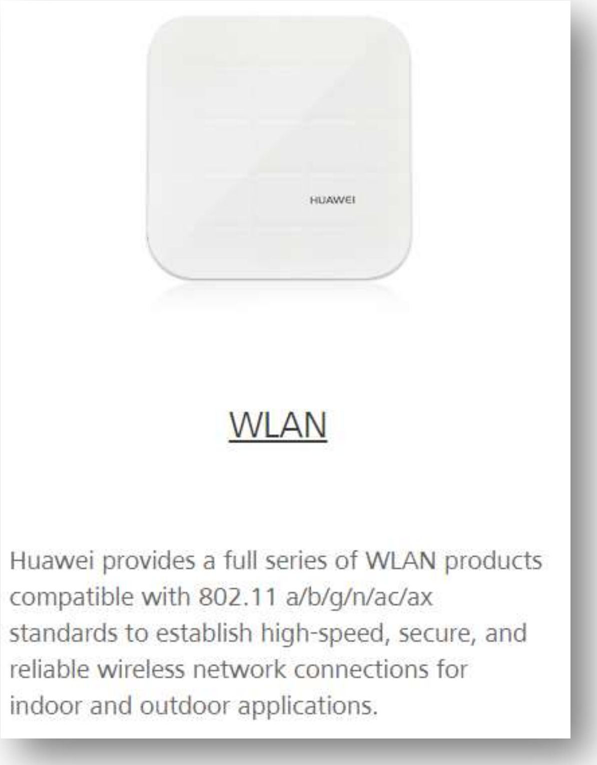
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	- Act as major partners of Huawei's Enterprise BG in regional markets. - Promise to accomplish business targets for related industries and customers of Huawei's Enterprise BG. - Develop industry customer relationship platforms and provide support for Huawei's products to industry users. https://e.huawei.com/en/partner/partner-program/policy Huawei also has more than 50 Authorized Partners that offer Enterprise Network products *See* https://e.huawei.com/en/partner/find-a-partner Huawei further actively encourages infringement and sales of Huawei networks by imposing penalties for violations: "Level-2 violation" of the partnership agreement to "direct unauthorized sales" "Level-3 violation" for "indirect unauthorized sales" and if a "Channel does not fulfill service contract or order" or "Provides services to customers through non-Huawei certified maintenance companies" Channel Partner Program Briefing 2018 at p.9, available at https://e.huawei.com/en/marketing-material/partner-document/partner/en/policy/20170428113204
[a] a plurality of stations for transmitting data in packets each having a packet type associated therewith; and	Huawei '690 Patent Accused Products comprise a plurality of stations (including, without limitation, Stations, STAs, Access Points, APs, and/or Remote Units) for transmitting data in packets each having a packet type associated therewith. One exemplary configuration is shown:

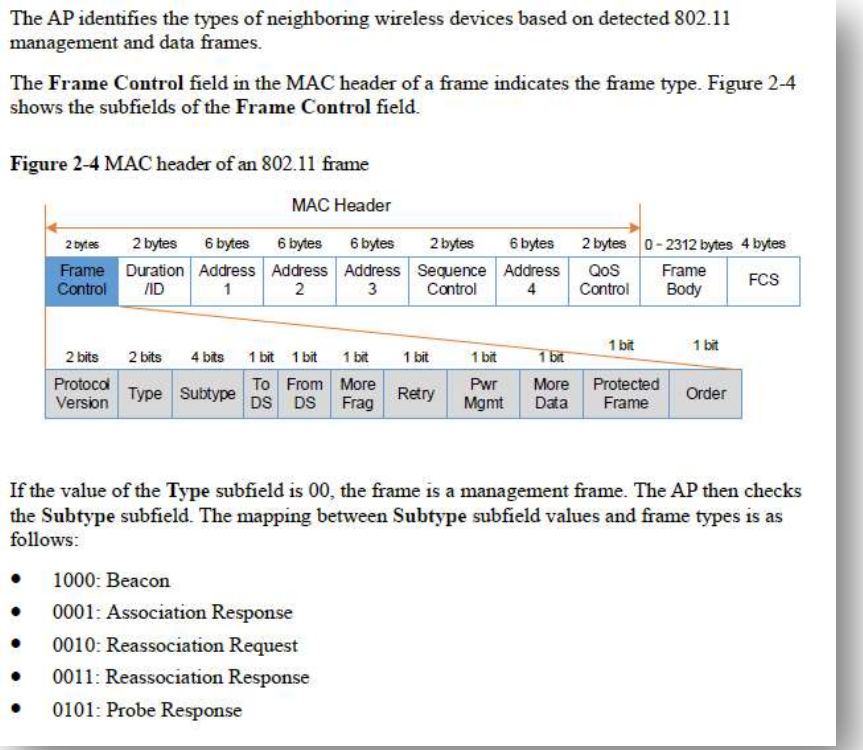
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 **WLAN Infrastructure** Figure 1-1 WLAN Networking RADIUS Server MAN NMS AC CAPWAP tunnel Aggregation switch Data flow Management flow Access switch AP AC CAPWAP tunnel Aggregation switch Data flow Management flow Access switch AP Aggregation switch Data flow CAPWAP tunnel AC Management flow Access switch AP Chain networking (tunnel forwarding) Chain networking (direct forwarding) Branched networking (direct forwarding)

’690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 As shown in Figure 1-1, a WLAN consists of access points (APs), PoE switches, access controllers (ACs), Remote Authentication Dial In User Service (RADIUS) server, and network management system (NMS). - AP: WLAN access device. Huawei provides a series of fit APs to meet indoor and outdoor networking requirements. - PoE switch: upstream devices for APs. It provides data switching and power for APs. If only one AC is required and the AC has PoE ports, the PoE switch is not required. - AC: manages APs and controls the rights of WLAN users. - RADIUS server: authenticates WLAN users and assigns rights to them. The RADIUS server is installed on the SPES server. - NMS: manages APs and ACs. It monitors status of ACs and APs in real time, processes alarms, and analyzes data. HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 2. https://support.huawei.com/enterprise/en/doc/EDOC1000184389/1d542042/introduction-to-wlan In another configuration example, a WDS (Wireless Distribution System) may wirelessly connect two WLANs:

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 1-1 WDS network  AP3 (leaf) AP2 (middle) AP1 (root) AC STA STA Switch S WDS network STA L2 network WVL Service VAP Huawei Technologies Co., Ltd. WLAN WDS Technology White Paper Issue 03 (2017-11-21) at 1-2. For example, Huawei WLAN products communicate using the IEEE 802.11 standards, which provide for transmitting data in packets with packet types associated therewith. Huawei 802.11ac APs are backwards compatible with 802.11a/b/g/n standards, 802.11ac APs enable existing networks to easily migrate to 802.11ac networks.

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	[As of 2014, for enterprise networks of different types and scales, Huawei offers the following AP models: 802.11ac indoor 7X30 series and 5X30 series APs, outdoor 802.11ac 8X30 series APs, and 802.11ac AP9130DN vehicle-mounted APs specially designed for rail transit communications. Huawei Enterprise AP Series 802.11ac Brochure, 2014, at 2. *See also*: 3.2 Data Packet Processing Packets transmitted on a WLAN include management packets and service data packets. Management packets must be transmitted over Control and Provisioning of Wireless Access Points (CAPWAP) tunnels, and service data packets can be transmitted over CAPWAP tunnels, soft GRE tunnels, or directly. Management packets transmit management data between an AC and AP. Data packets transmit data from STAs and the upper-layer network when WLAN users surf on the Internet. On a WLAN, packets transmitted between STAs and APs are 802.11 packets… Huawei, Typical Configuration Examples, Issue 01 (2017-12-29) at 38.

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 WLAN Huawei provides a full series of WLAN products compatible with 802.11 a/b/g/n/ac/ax standards to establish high-speed, secure, and reliable wireless network connections for indoor and outdoor applications. https://e.huawei.com/en/solutions/business-needs/enterprise-network/campus-network/cloudcampus/cloud-managed-network

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	

The AP identifies the types of neighboring wireless devices based on detected 802.11 management and data frames.

The **Frame Control** field in the MAC header of a frame indicates the frame type. Figure 2-4 shows the subfields of the **Frame Control** field.

Figure 2-4 MAC header of an 802.11 frame

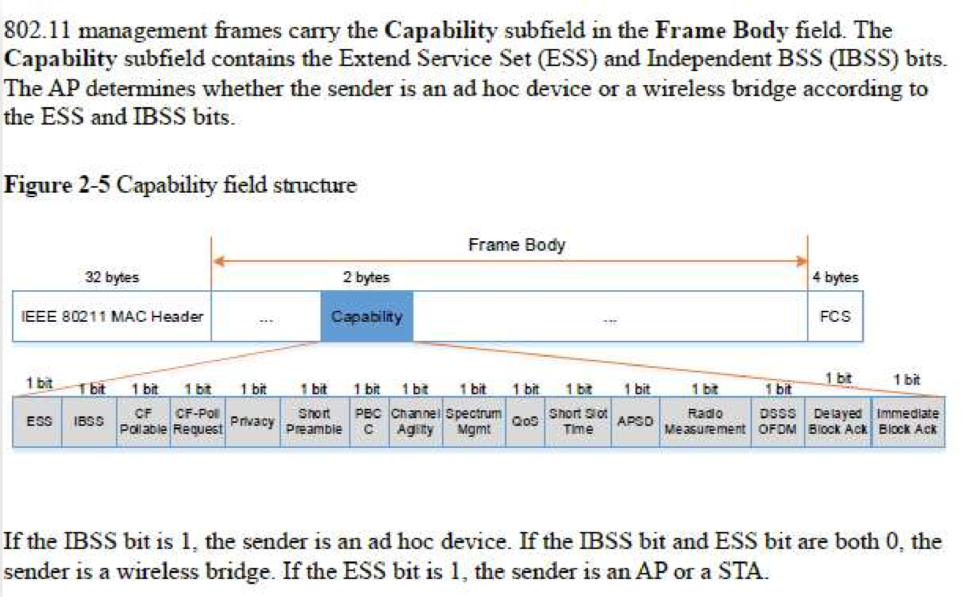
MAC Header

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	2 bytes	0 - 2312 bytes	4 bytes
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	Frame Body	FCS

2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	Protected Frame	Order

If the value of the **Type** subfield is 00, the frame is a management frame. The AP then checks the **Subtype** subfield. The mapping between **Subtype** subfield values and frame types is as follows:

- 1000: Beacon
- 0001: Association Response
- 0010: Reassociation Request
- 0011: Reassociation Response
- 0101: Probe Response

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 802.11 management frames carry the **Capability** subfield in the **Frame Body** field. The **Capability** subfield contains the Extend Service Set (ESS) and Independent BSS (IBSS) bits. The AP determines whether the sender is an ad hoc device or a wireless bridge according to the ESS and IBSS bits. **Figure 2-5** Capability field structure Frame Body 32 bytes 2 bytes 4 bytes IEEE 80211 MAC Header ... Capability ... FCS 1 bit ESS IBSS CF Pollable CF-Poll Request Privacy Short Preamble PBC C Channel Agility Spectrum Mgmt QoS Short Slot Time APSD Radio Measurement DSSS OFDM Delayed Block Ack Immediate Block Ack If the IBSS bit is 1, the sender is an ad hoc device. If the IBSS bit and ESS bit are both 0, the sender is a wireless bridge. If the ESS bit is 1, the sender is an AP or a STA.

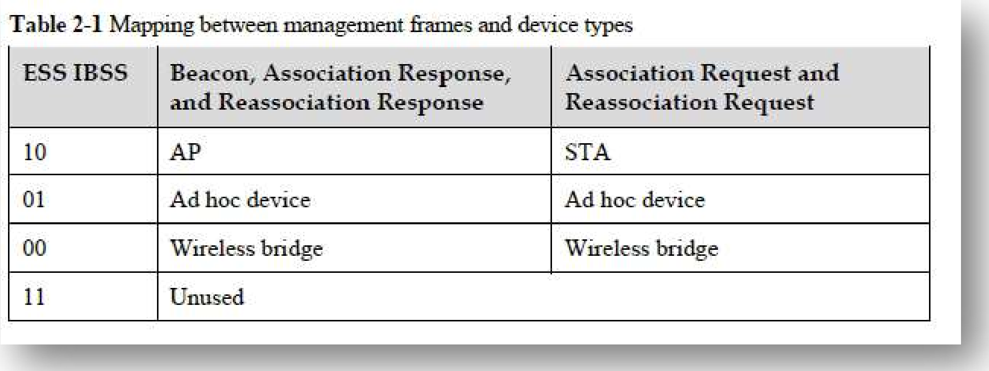
<table>
<tr><th>'690 PATENT CLAIM 32</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>


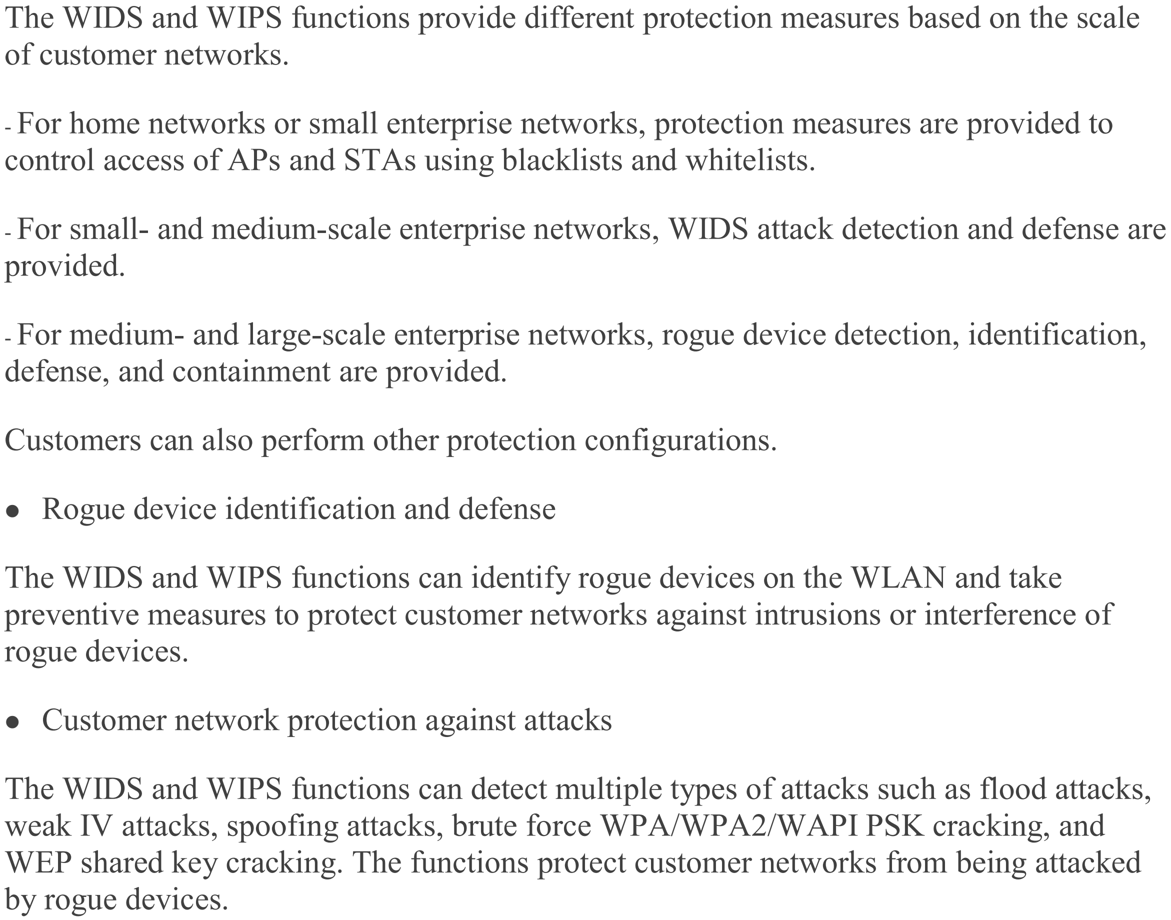
Table 2-1 Mapping between management frames and device types

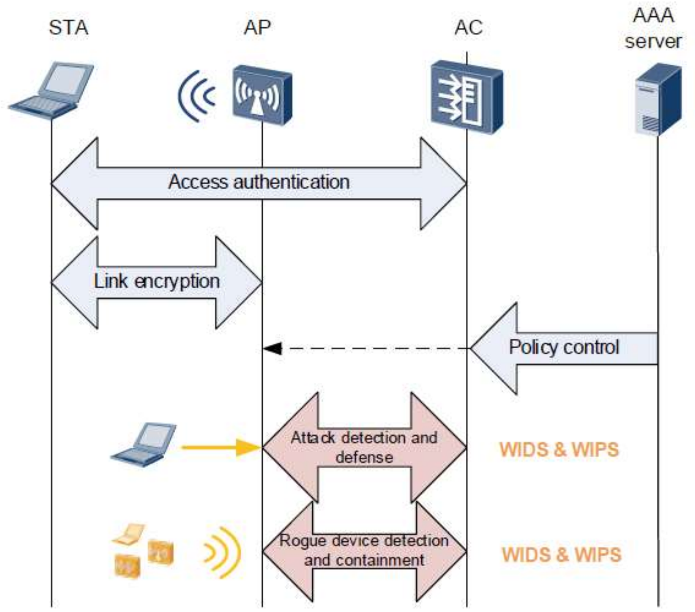
<table>
<tr><th>ESS IBSS</th><th>Beacon, Association Response, and Reassociation Response</th><th>Association Request and Reassociation Request</th></tr>
<tr><td>10</td><td>AP</td><td>STA</td></tr>
<tr><td>01</td><td>Ad hoc device</td><td>Ad hoc device</td></tr>
<tr><td>00</td><td>Wireless bridge</td><td>Wireless bridge</td></tr>
<tr><td>11</td><td>Unused</td><td></td></tr>
</table>

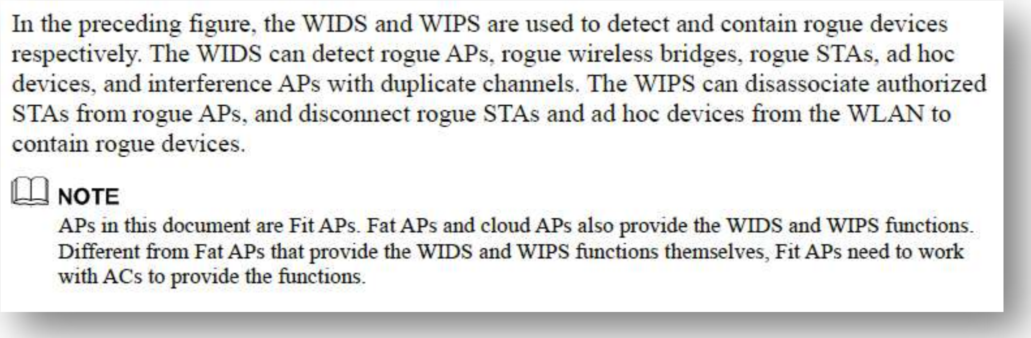
Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 5-6; *see also* WLAN WIDS Technology White Paper, Issue 1 (2014-04-24) at 4-7.

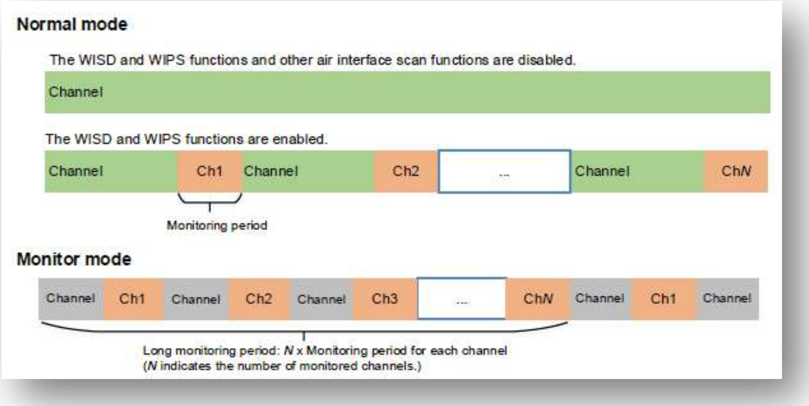
Huawei consumer devices, including laptops, phones and tablets, also participate in the WIDS system as client stations (also referred to in WIDS and documentation as "STAs" or "ad hoc" devices) that transmit data in packets each having a packet type. *See, e.g.*, Huawei Technologies Co., Ltd., *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 7 ("When receiving a Probe Request, an Association Request, or a Reassociation Request frame, the AP determines whether the sender is an ad hoc device or STA based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame") *see also id.* at 11 ("Rogue STAs: After detecting a rogue STA, a monitor AP uses the BSSID and MAC address of the rogue STA to send a fake unicast Deauthentication frame to contain it. A STA whitelist can also be configured to prevent STAs in the STA whitelist from associating with rogue APs").
</td></tr>
</table>

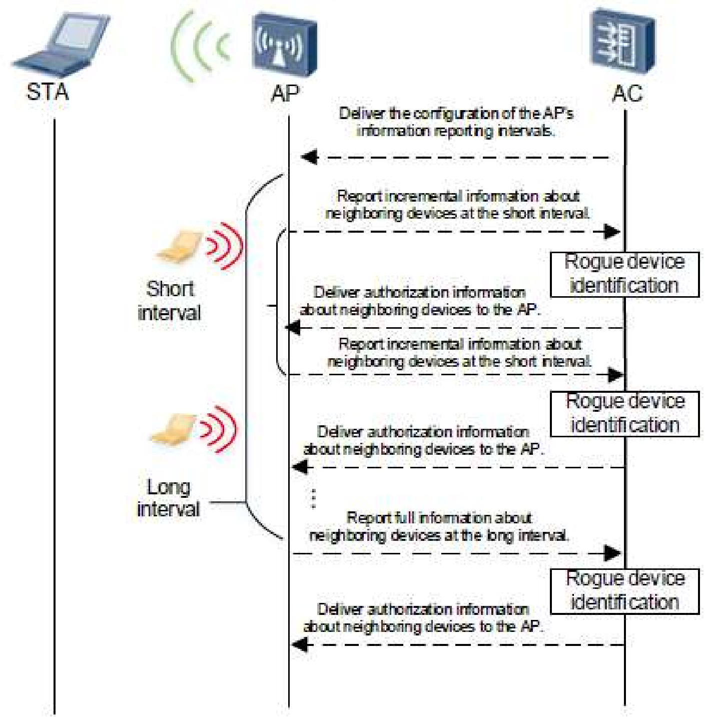
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
[b] a policing station for detecting intrusions into the wireless network by	Huawei '690 Patent Accused Products comprise a policing station for detecting intrusions into the wireless network. For example, Huawei WLAN products utilize the WIDS technology to detect intrusions 802.11 networks are open wireless public networks, and vulnerable to various threats caused by unauthorized APs and STAs, ad hoc networks, bogus APs, and denial of service (DoS) attacks of malicious STAs. The Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions monitor and prevent the preceding attacks on WLANs. This document describes WIDS and WIPS technologies used by Huawei WLAN products. Enterprises can use the WIDS and WIPS functions to secure their wireless networks, reduce interference from unauthorized devices, protect STAs from malicious attacks, and deliver better user experience. … The WIDS detects rogue STAs, malicious user attacks, and wireless network intrusions. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 1-2. The WIDS and WIPS functions of Huawei WLAN products ensure security of customers' wireless networks, reduce interference from rogue devices, and protect STAs from malicious attacks, delivering better user experience. ● Selection of different protection measures based on their network scale

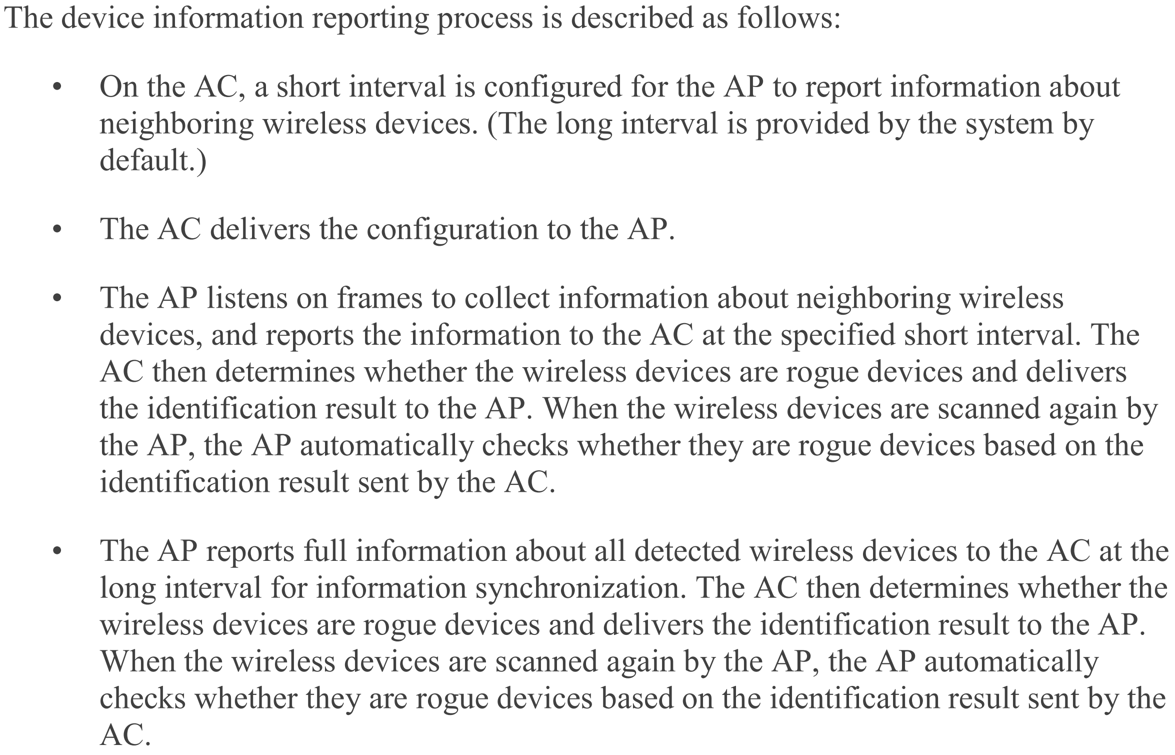
'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	 The WIDS and WIPS functions provide different protection measures based on the scale of customer networks. - For home networks or small enterprise networks, protection measures are provided to control access of APs and STAs using blacklists and whitelists. - For small- and medium-scale enterprise networks, WIDS attack detection and defense are provided. - For medium- and large-scale enterprise networks, rogue device detection, identification, defense, and containment are provided. Customers can also perform other protection configurations. ● Rogue device identification and defense The WIDS and WIPS functions can identify rogue devices on the WLAN and take preventive measures to protect customer networks against intrusions or interference of rogue devices. ● Customer network protection against attacks The WIDS and WIPS functions can detect multiple types of attacks such as flood attacks, weak IV attacks, spoofing attacks, brute force WPA/WPA2/WAPI PSK cracking, and WEP shared key cracking. The functions protect customer networks from being attacked by rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 20.

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	For example, a monitor AP may act as a policing station for detecting intrusions (e.g., rogue devices) into the wireless network: **Figure 2-1** Overview of WLAN security technologies  STA AP AC AAA server Access authentication Link encryption Policy control Attack detection and defense WIDS & WIPS Rogue device detection and containment WIDS & WIPS

’690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 In the preceding figure, the WIDS and WIPS are used to detect and contain rogue devices respectively. The WIDS can detect rogue APs, rogue wireless bridges, rogue STAs, ad hoc devices, and interference APs with duplicate channels. The WIPS can disassociate authorized STAs from rogue APs, and disconnect rogue STAs and ad hoc devices from the WLAN to contain rogue devices. NOTE APs in this document are Fit APs. Fat APs and cloud APs also provide the WIDS and WIPS functions. Different from Fat APs that provide the WIDS and WIPS functions themselves, Fit APs need to work with ACs to provide the functions. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3. 2.2 Rogue Device Detection Rogue device detection of WLANs is enabled to monitor the entire network. Monitor APs are deployed on a WLAN that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless signals to detect rogue devices. 2.2.1 Working Modes of APs Before enabling rogue device detection on a WLAN, configure APs' working modes. An AP works in normal or monitor mode. • Normal mode: If the WIDS and WIPS functions and other air interface scan functions are disabled on a radio, such as spectrum analysis and STA location, this radio can be used only to transmit common WLAN service data. If the WIDS and

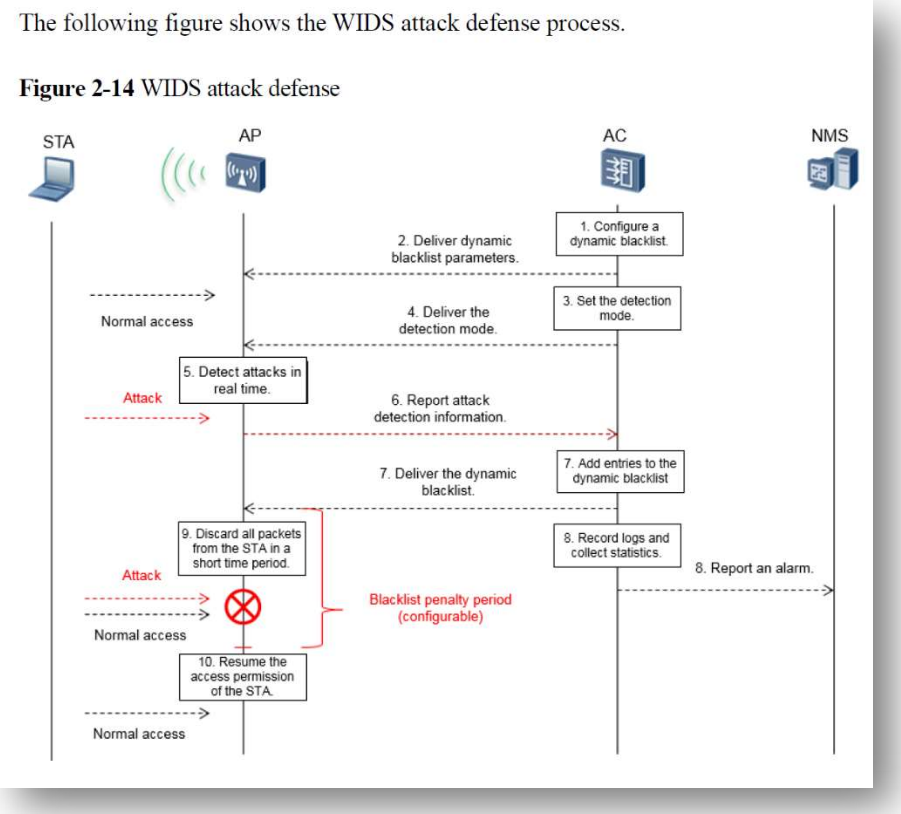
’690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	WIPS functions are enabled, the working mode of the radio is automatically switched to hybrid. In addition to transmitting common WLAN service data, the radio can also provide the monitoring function. In this case, transmission of common WLAN service data is affected. • Monitor mode: A monitor AP scans devices on the WLAN and listens on all 802.11 frames on wireless channels. In this case, the monitor AP provides only the monitoring function and cannot transmit WLAN service data. The following figure shows the principles of the two working modes.  Normal mode The WISD and WIPS functions and other air interface scan functions are disabled. Channel The WISD and WIPS functions are enabled. Channel Ch1 Channel Ch2 ... Channel ChN Monitoring period Monitor mode Channel Ch1 Channel Ch2 Channel Ch3 ... ChN Channel Ch1 Channel Long monitoring period: N x Monitoring period for each channel (N indicates the number of monitored channels.) Figure 2-2 Principles of the two working modes

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 2-6 Device information reporting process  STA AP AC Deliver the configuration of the AP's information reporting intervals. Report incremental information about neighboring devices at the short interval. Rogue device identification Short interval Deliver authorization information about neighboring devices to the AP. Report incremental information about neighboring devices at the short interval. Rogue device identification Deliver authorization information about neighboring devices to the AP. Long interval Report full information about neighboring devices at the long interval. Rogue device identification Deliver authorization information about neighboring devices to the AP. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3-4.

’690 Patent Claim 32	Infringement By Huawei Corporation
	 The device information reporting process is described as follows: • On the AC, a short interval is configured for the AP to report information about neighboring wireless devices. (The long interval is provided by the system by default.) • The AC delivers the configuration to the AP. • The AP listens on frames to collect information about neighboring wireless devices, and reports the information to the AC at the specified short interval. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC. • The AP reports full information about all detected wireless devices to the AC at the long interval for information synchronization. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 8.

<table>
<tr><th>'690 PATENT CLAIM 32</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

See also:



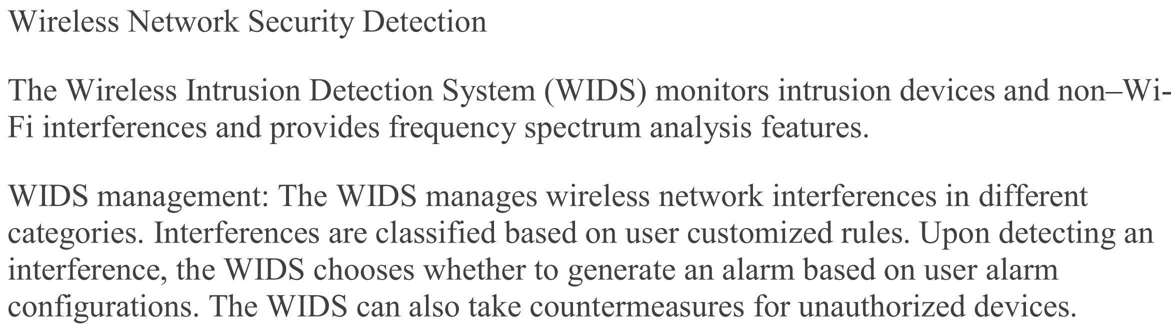
The following figure shows the WIDS attack defense process.

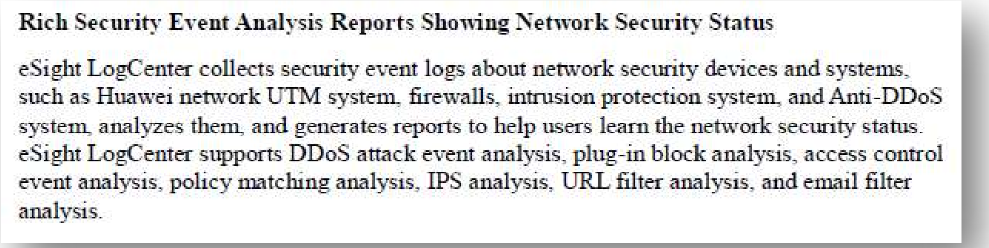
Figure 2-14 WIDS attack defense

STA
AP
AC
NMS
1. Configure a dynamic blacklist.
2. Deliver dynamic blacklist parameters.
Normal access
3. Set the detection mode.
4. Deliver the detection mode.
5. Detect attacks in real time.
Attack
6. Report attack detection information.
7. Add entries to the dynamic blacklist
7. Deliver the dynamic blacklist.
9. Discard all packets from the STA in a short time period.
Attack
8. Record logs and collect statistics.
8. Report an alarm.
Blacklist penalty period (configurable)
Normal access
10. Resume the access permission of the STA.
Normal access

Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 17.

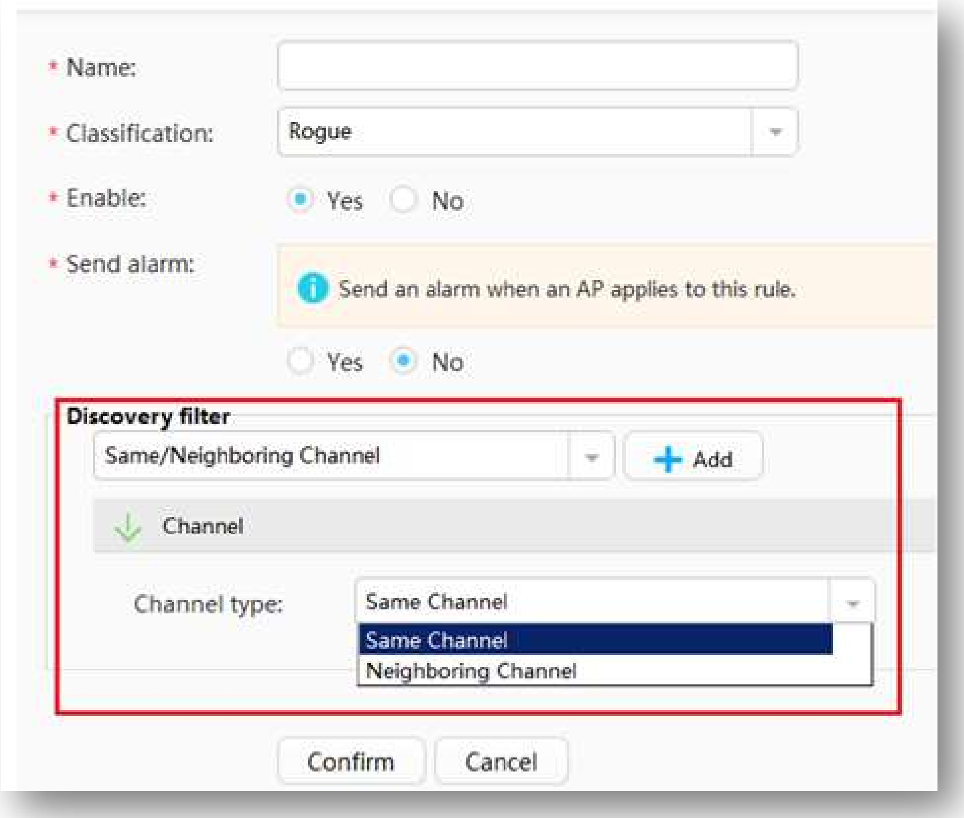
</td></tr>
</table>

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	The Huawei eSight Platform, including at least the WLAN Manager and LogCenter Manager, is further used as a network management system that also detects intrusions into the wireless network**:** The Huawei eSight Platform further incorporates the WIDS system:  Wireless Network Security Detection The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non–Wi-Fi interferences and provides frequency spectrum analysis features. WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices. Huawei eSight Full Product Datasheet, CH 12 eSight WLAN Manager; p. 53 (2013-09-03) Huawei Technologies Co., Ltd.; *see also* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 58-59 (indicating that, on information and belief, all versions of eSight incorporate WIDS).

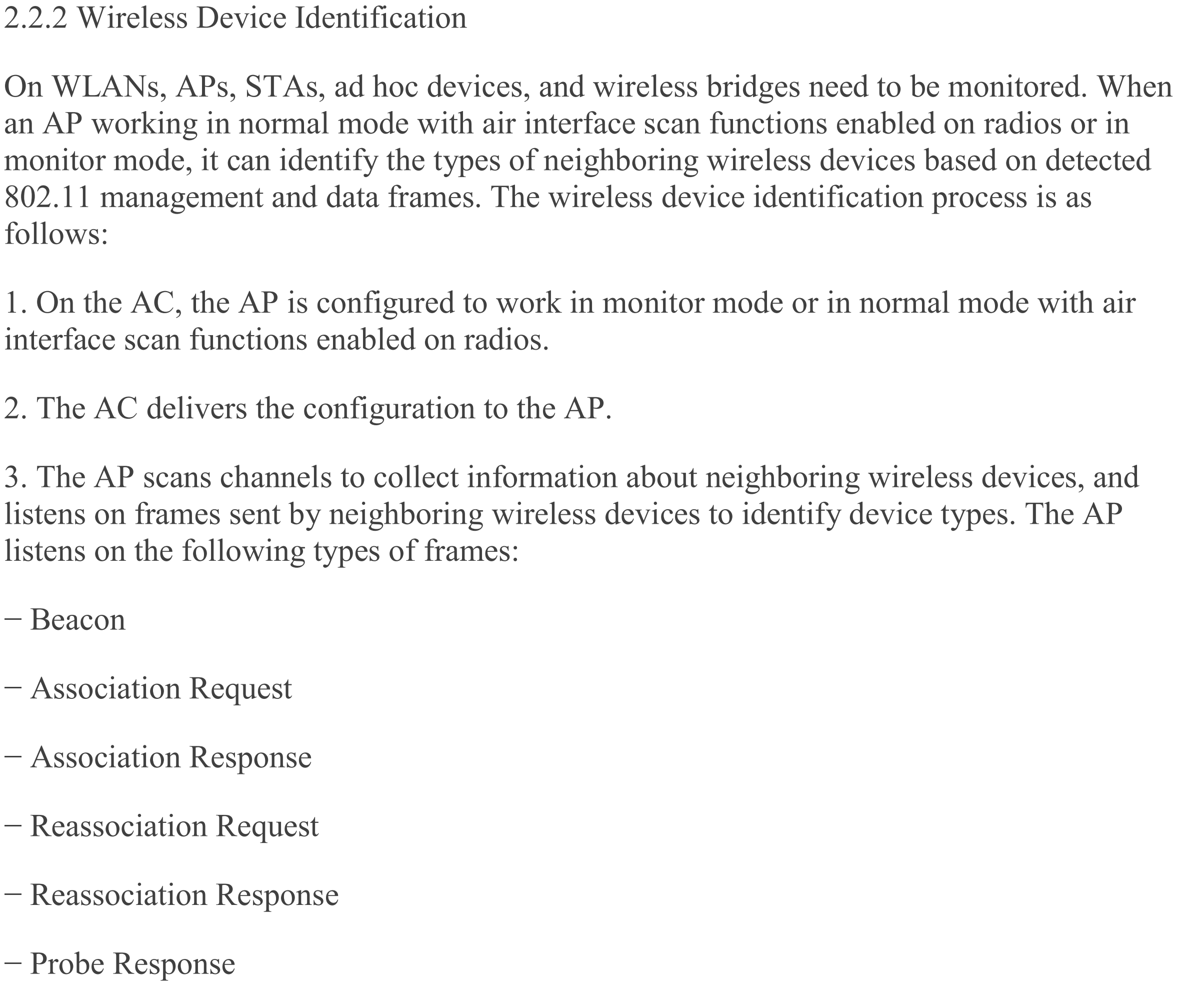
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 **Rich Security Event Analysis Reports Showing Network Security Status** eSight LogCenter collects security event logs about network security devices and systems, such as Huawei network UTM system, firewalls, intrusion protection system, and Anti-DDoS system, analyzes them, and generates reports to help users learn the network security status. eSight LogCenter supports DDoS attack event analysis, plug-in block analysis, access control event analysis, policy matching analysis, IPS analysis, URL filter analysis, and email filter analysis. Huawei eSight Full Product Datasheet, CH 11 eSight LogCenter Manager; p. 44 (2013-09-03) Security Users can monitor rogue devices, clients, interference sources, and attacks on the network, define rules to identify intrusion devices, generate remote alarm notifications, and take measures to prevent intrusions. 1. Supports statistics and display of and countermeasure against rogue devices. 2. Supports the display of and countermeasure against rogue clients and suppression access protection. 3. Supports statistics and display of non-Wi-Fi interference sources. 4. Supports statistics and display of attacks and protection against attacks. 5. Allows users to define rules and classify rogue APs (rogue, suspected-rogue, adjacent, suspected-adjacent, and interference). Supported rule matching indicators include

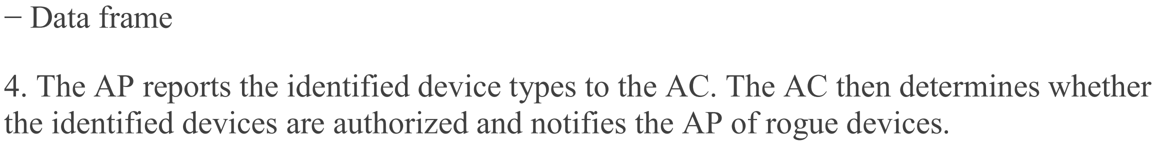
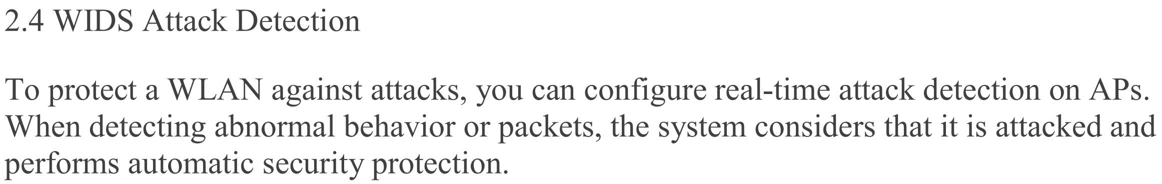
'690 Patent Claim 32	**Infringement By Huawei Corporation**
	adjacent- or same-frequency interference, signal strength, SSID (fuzzy match/regular expression), the number of detected APs, and whether to attack. eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 63. On information and belief Huawei consumer devices, including laptops, phones and tablets also can participate in the WIDS system as access points ("APs"), including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also implement intrusion detection according to the claim. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").
[c] monitoring transmissions among said plurality of stations to detect collisions of packets having a predetermined packet type; and	Huawei '690 Patent Accused Products comprise policing stations, as described above in [b], that are capable of detecting intrusions by monitoring transmissions among said plurality of stations to detect collisions of packets having a predetermined packet type. For example, as described in eSight documentation, the WIDS monitors transmissions among the stations: WIDS Wireless Intrusion Detection System The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm

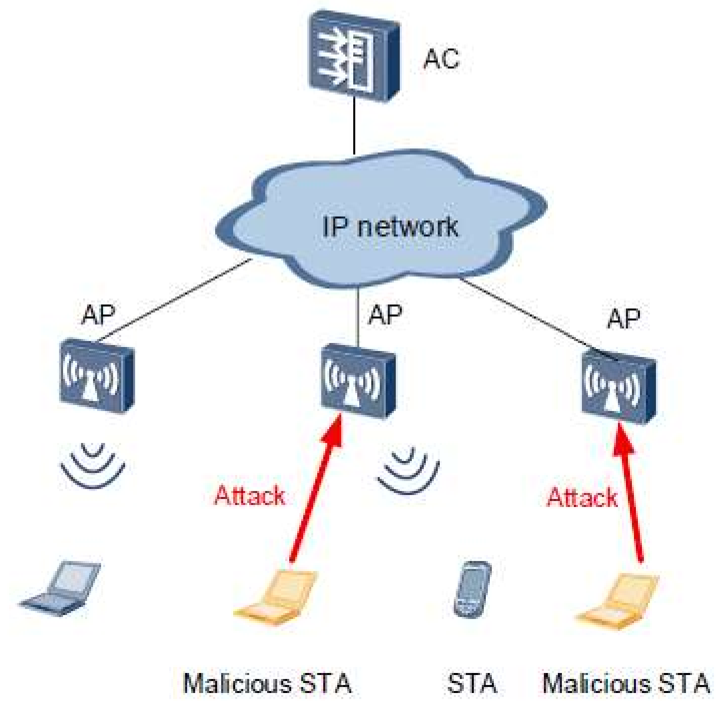
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security. … Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. Same or adjacent channel This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference

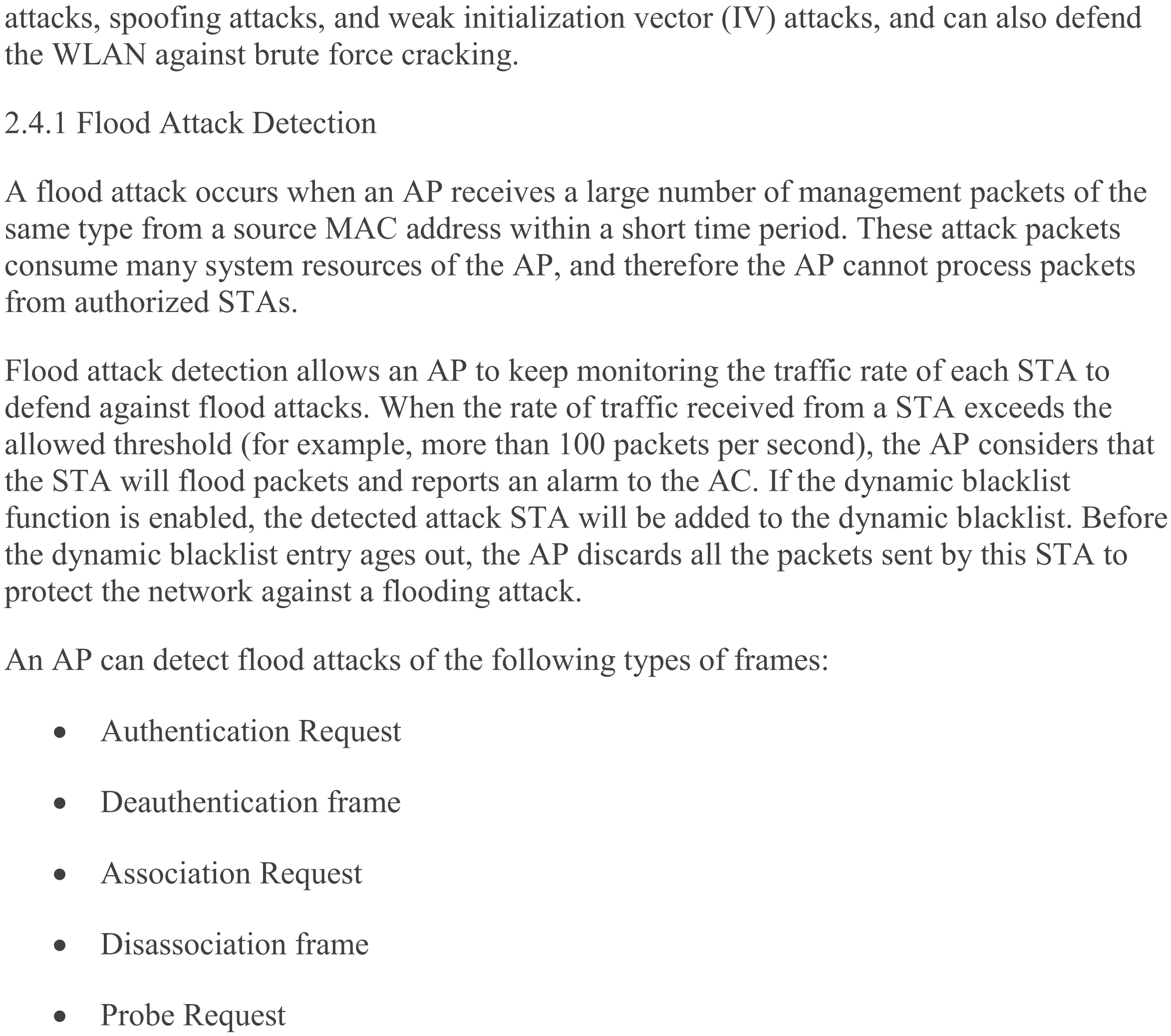
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 * Name: * Classification: Rogue * Enable: ● Yes ○ No * Send alarm: Send an alarm when an AP applies to this rule. ○ Yes ● No Discovery filter Same/Neighboring Channel Channel Channel type: Same Channel Same Channel Neighboring Channel HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12. For example, monitor APs may monitor network or neighboring devices and detect transmissions of neighboring wireless devices to detect collisions of packets having a predetermined packet type:

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Rogue AP: an unauthorized or malicious AP, which can be an AP that is connected to a network without permission, an unconfigured AP, a neighbor AP, or an AP manipulated by an attacker … Monitor AP: an AP that scans or listens on wireless channels and attempts to detect attacks to the wireless network. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 2; *see also* WLAN WIDS Technology White Paper, Issue 1.0 (2014-04-24) at 3. 2.2 Rogue Device Detection Rogue device detection of WLANs is enabled to monitor the entire network. Monitor APs are deployed on a WLAN that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless signals to detect rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 3. After the WIDS and WIPS functions are configured on the AC, the monitor AP collects information about neighboring device and reports the information to the AC. When the AC identifies a rogue AP, it notifies the monitor AP of the rogue AP's identity information. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 22. Further, the AP monitors transmissions and detects collisions of packets having a predetermined packet type:

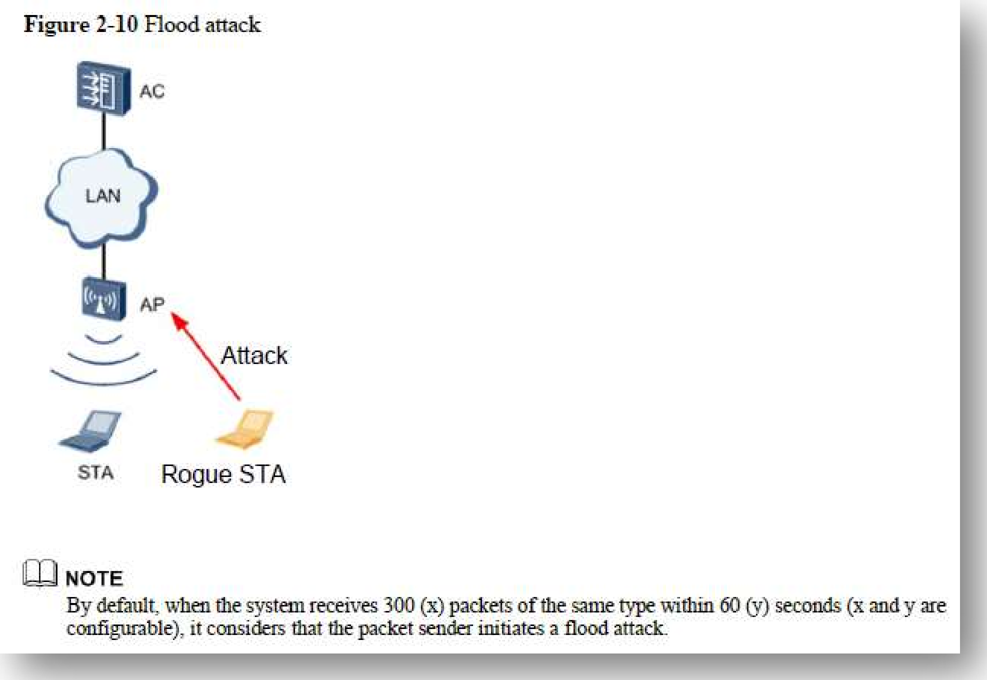
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 2.2.2 Wireless Device Identification On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows: 1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios. 2. The AC delivers the configuration to the AP. 3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames: – Beacon – Association Request – Association Response – Reassociation Request – Reassociation Response – Probe Response

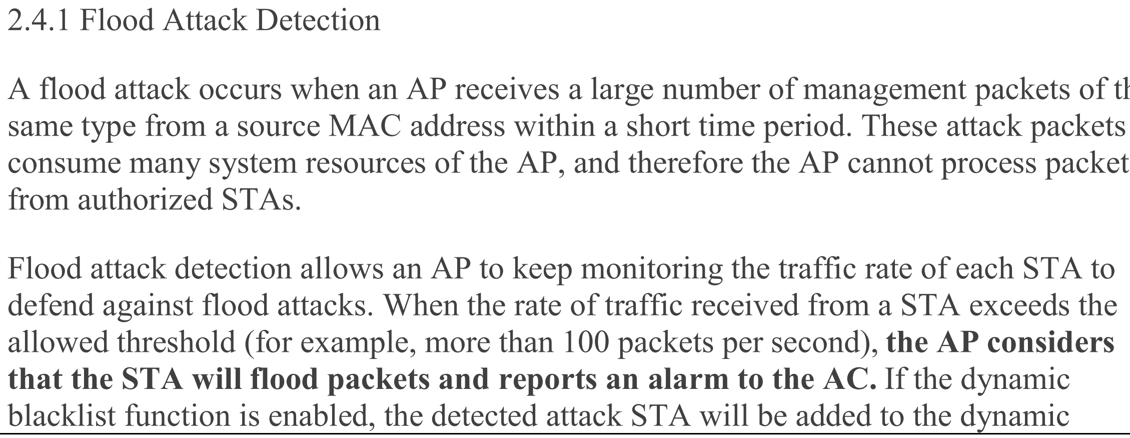
'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	 – Data frame 4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4.  2.4 WIDS Attack Detection To protect a WLAN against attacks, you can configure real-time attack detection on APs. When detecting abnormal behavior or packets, the system considers that it is attacked and performs automatic security protection.

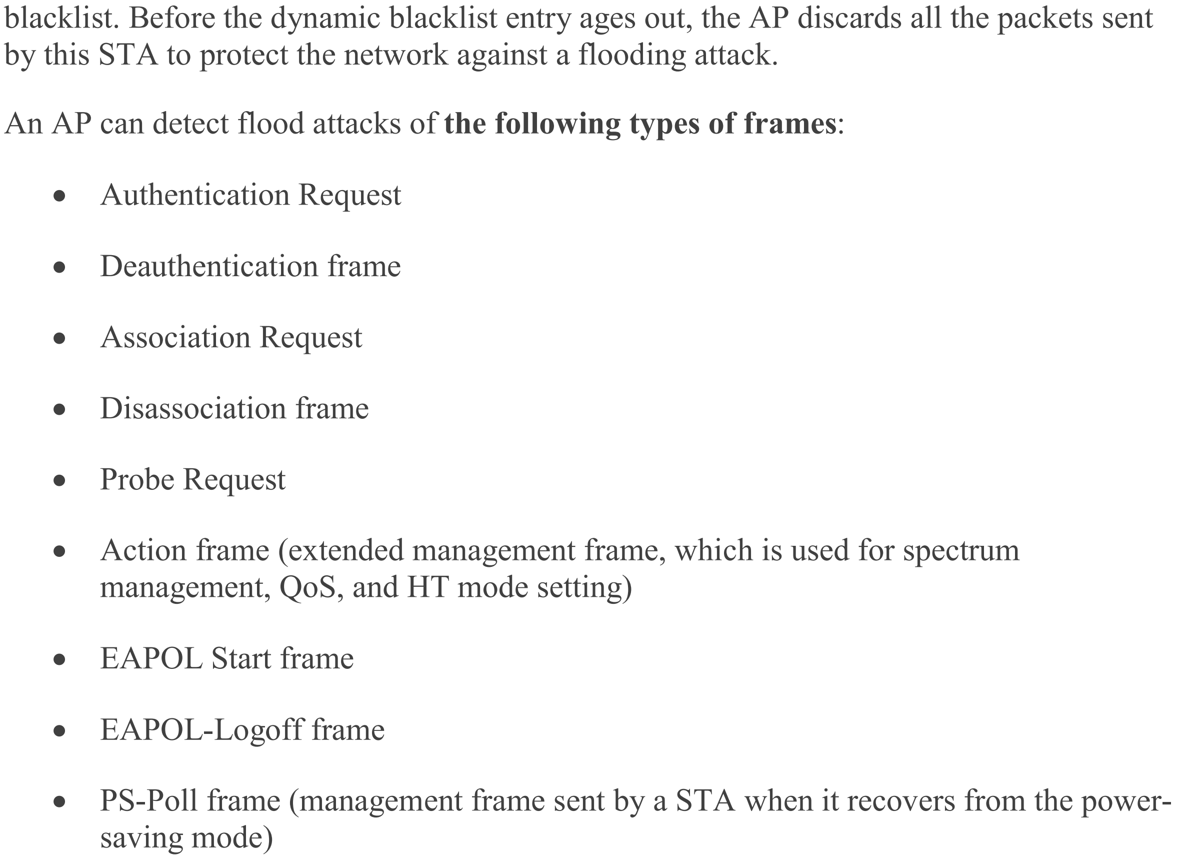
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 2-9 WIDS attack detection scenario  AC IP network AP AP AP Attack Attack Malicious STA STA Malicious STA On the WLAN shown in the preceding figure, WIDS attack detection can be enabled on the AC when the WLAN access service is provided. The WIDS can detect 802.11 flood

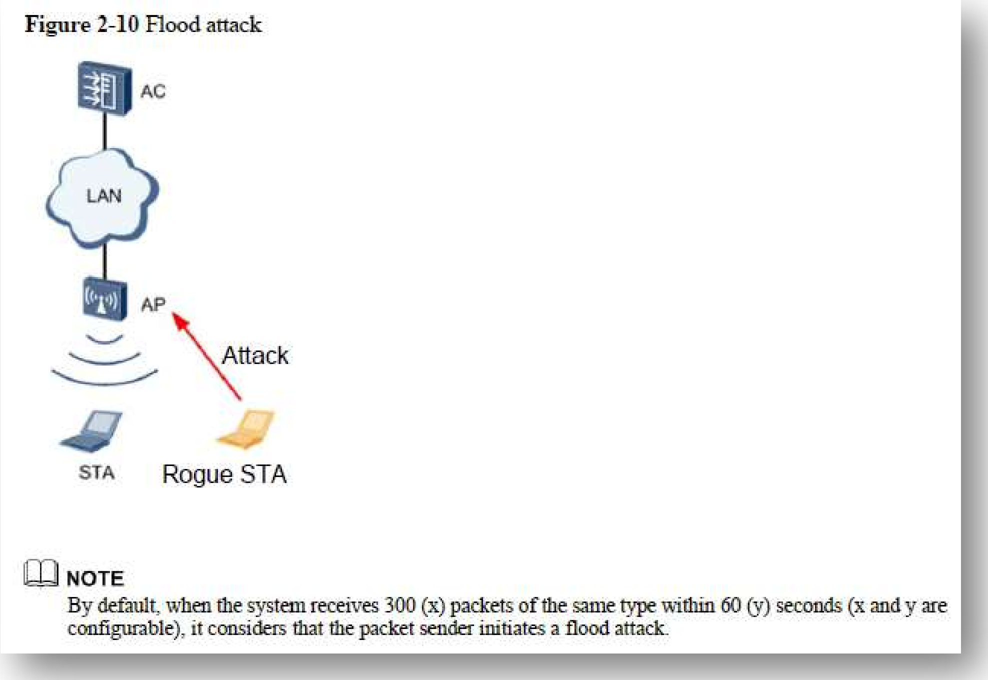
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 attacks, spoofing attacks, and weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking. 2.4.1 Flood Attack Detection A flood attack occurs when an AP receives a large number of management packets of the same type from a source MAC address within a short time period. These attack packets consume many system resources of the AP, and therefore the AP cannot process packets from authorized STAs. Flood attack detection allows an AP to keep monitoring the traffic rate of each STA to defend against flood attacks. When the rate of traffic received from a STA exceeds the allowed threshold (for example, more than 100 packets per second), the AP considers that the STA will flood packets and reports an alarm to the AC. If the dynamic blacklist function is enabled, the detected attack STA will be added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the AP discards all the packets sent by this STA to protect the network against a flooding attack. An AP can detect flood attacks of the following types of frames: • Authentication Request • Deauthentication frame • Association Request • Disassociation frame • Probe Request

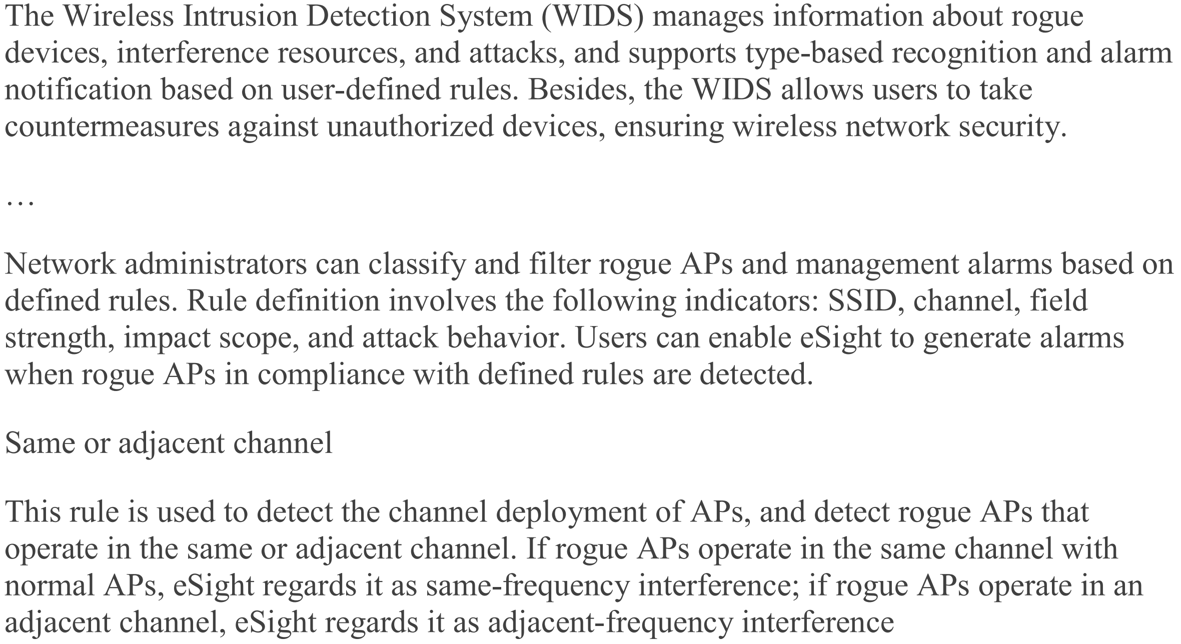
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	• Action frame (extended management frame, which is used for spectrum management, QoS, and HT mode setting) • EAPOL Start frame • EAPOL-Logoff frame • PS-Poll frame (management frame sent by a STA when it recovers from the power-saving mode)

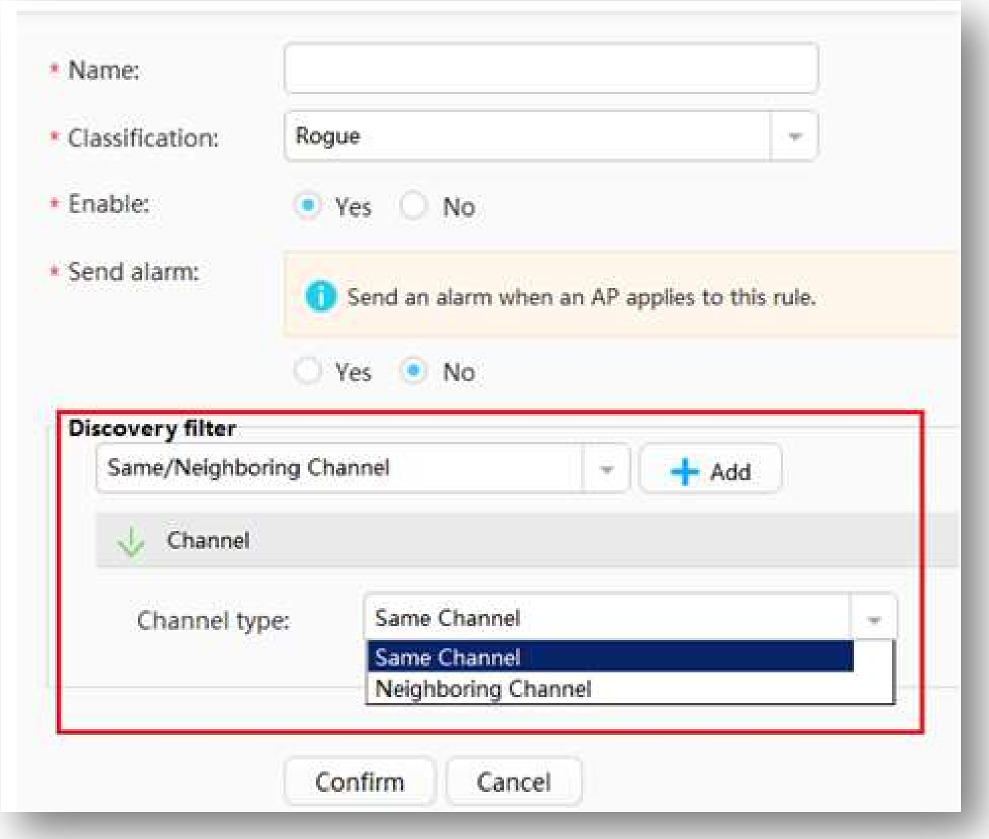
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Figure 2-10 Flood attack NOTE By default, when the system receives 300 (x) packets of the same type within 60 (y) seconds (x and y are configurable), it considers that the packet sender initiates a flood attack. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12-13. On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for collisions of packets of a predetermined type, including when configured as a mobile hotspot.

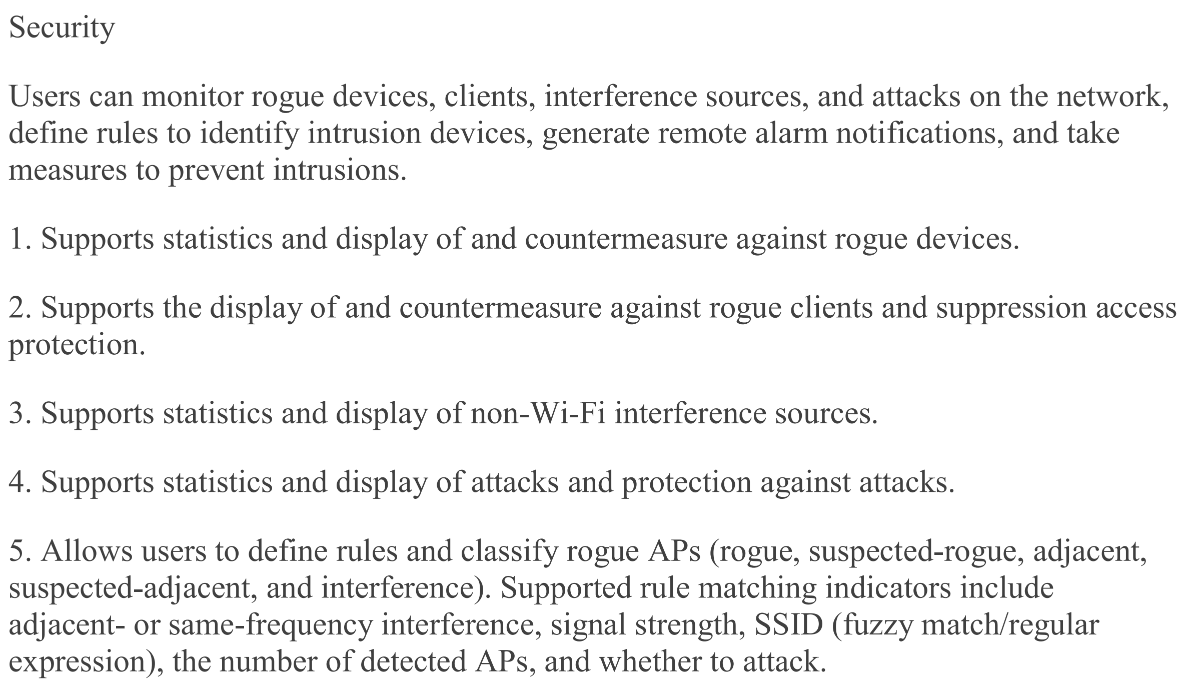
'690 Patent Claim 32	Infringement By Huawei Corporation
	Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also monitor for collisions of packets of a predetermined type. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").
[d] generating an intrusion alert based upon detecting a threshold number of collisions of packets having the predetermined packet type.	In the Huawei '690 Patent Accused Products, the policing station is capable of generating an intrusion alert based upon detecting a threshold number of collisions of packets having the predetermined packet type. For example, collisions of predetermined packet types may include the packet types described below:  2.4.1 Flood Attack Detection A flood attack occurs when an AP receives a large number of management packets of the same type from a source MAC address within a short time period. These attack packets consume many system resources of the AP, and therefore the AP cannot process packets from authorized STAs. Flood attack detection allows an AP to keep monitoring the traffic rate of each STA to defend against flood attacks. When the rate of traffic received from a STA exceeds the allowed threshold (for example, more than 100 packets per second), **the AP considers that the STA will flood packets and reports an alarm to the AC.** If the dynamic blacklist function is enabled, the detected attack STA will be added to the dynamic

’690 Patent Claim 32	Infringement By Huawei Corporation
	 blacklist. Before the dynamic blacklist entry ages out, the AP discards all the packets sent by this STA to protect the network against a flooding attack. An AP can detect flood attacks of **the following types of frames**: • Authentication Request • Deauthentication frame • Association Request • Disassociation frame • Probe Request • Action frame (extended management frame, which is used for spectrum management, QoS, and HT mode setting) • EAPOL Start frame • EAPOL-Logoff frame • PS-Poll frame (management frame sent by a STA when it recovers from the power-saving mode)

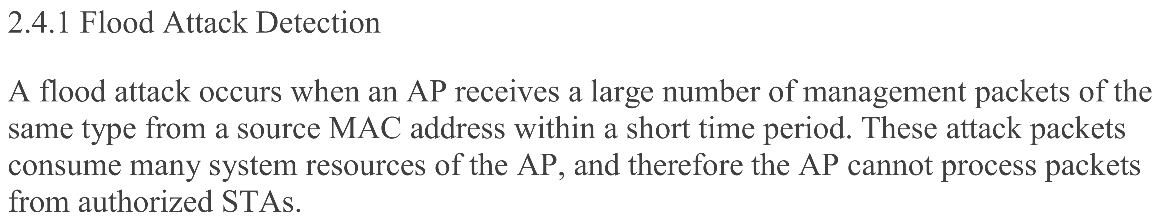
'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 Figure 2-10 Flood attack NOTE By default, when the system receives 300 (x) packets of the same type within 60 (y) seconds (x and y are configurable), it considers that the packet sender initiates a flood attack. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12-13 (emphasis added). An intrusion alert is also generated in the eSight system, for example: WIDS Wireless Intrusion Detection System

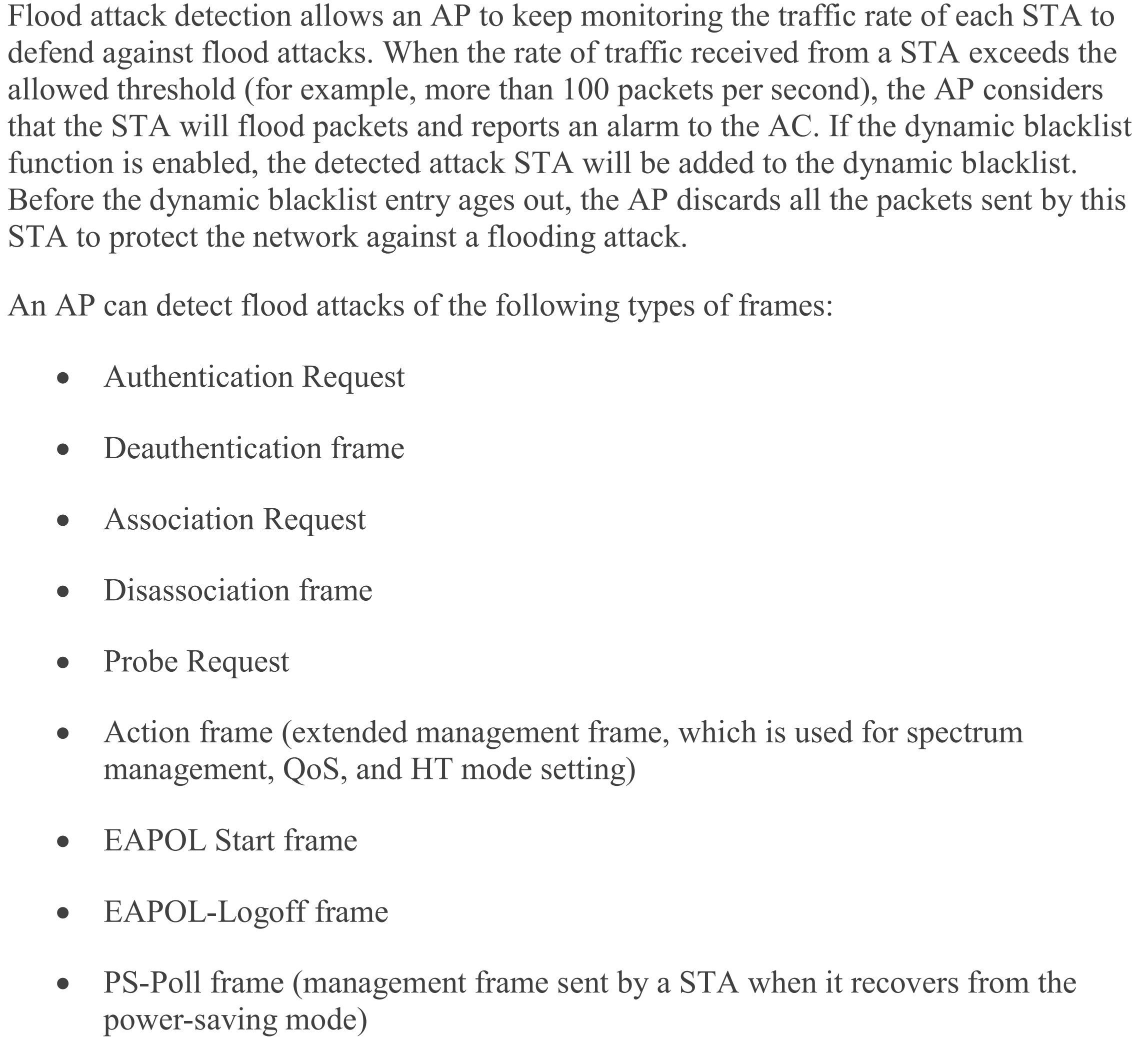
'690 Patent Claim 32	Infringement By Huawei Corporation
	The Wireless Intrusion Detection System (WIDS) manages information about rogue devices, interference resources, and attacks, and supports type-based recognition and alarm notification based on user-defined rules. Besides, the WIDS allows users to take countermeasures against unauthorized devices, ensuring wireless network security. … Network administrators can classify and filter rogue APs and management alarms based on defined rules. Rule definition involves the following indicators: SSID, channel, field strength, impact scope, and attack behavior. Users can enable eSight to generate alarms when rogue APs in compliance with defined rules are detected. Same or adjacent channel This rule is used to detect the channel deployment of APs, and detect rogue APs that operate in the same or adjacent channel. If rogue APs operate in the same channel with normal APs, eSight regards it as same-frequency interference; if rogue APs operate in an adjacent channel, eSight regards it as adjacent-frequency interference

'690 PATENT CLAIM 32	INFRINGEMENT BY HUAWEI CORPORATION
	 * Name: * Classification: Rogue * Enable: ● Yes ○ No * Send alarm: Send an alarm when an AP applies to this rule. ○ Yes ● No Discovery filter Same/Neighboring Channel + Add Channel Channel type: Same Channel Same Channel Neighboring Channel Confirm Cancel HUAWEI eSight WLAN Technology White Paper, Issue 01 (2017-03-20) at 10-12.

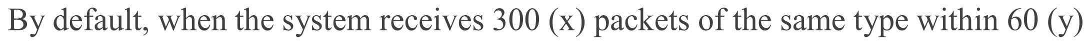
’690 Patent Claim 32	Infringement By Huawei Corporation
	 Security Users can monitor rogue devices, clients, interference sources, and attacks on the network, define rules to identify intrusion devices, generate remote alarm notifications, and take measures to prevent intrusions. 1. Supports statistics and display of and countermeasure against rogue devices. 2. Supports the display of and countermeasure against rogue clients and suppression access protection. 3. Supports statistics and display of non-Wi-Fi interference sources. 4. Supports statistics and display of attacks and protection against attacks. 5. Allows users to define rules and classify rogue APs (rogue, suspected-rogue, adjacent, suspected-adjacent, and interference). Supported rule matching indicators include adjacent- or same-frequency interference, signal strength, SSID (fuzzy match/regular expression), the number of detected APs, and whether to attack. eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at p. 63; *see also id.* at 74 (3. eSight supports alarms about communications, environments, rogue devices, non-Wi-Fi interference sources, and attacks to help users locate and resolve faults.). On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on monitoring for collisions of packets of a predetermined type, including when configured as a mobile hotspot.

'690 PATENT CLAIM 32	**INFRINGEMENT BY HUAWEI CORPORATION**
	Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also generate an intrusion alert based on monitoring for collisions of packets of a predetermined type. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

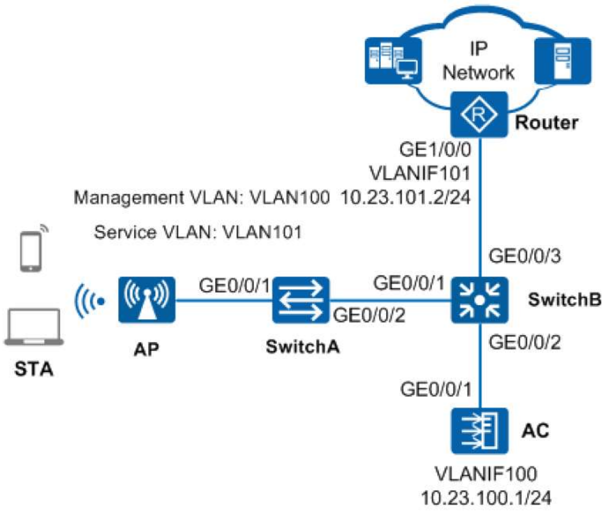
'690 PATENT CLAIM 33	**INFRINGEMENT BY HUAWEI CORPORATION**
33. The wireless network of claim 32 wherein the predetermined packet type comprises at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32. Further, the predetermined packet type described above in claim 32 further comprises at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets (for example, authentication and association packets):  2.4.1 Flood Attack Detection A flood attack occurs when an AP receives a large number of management packets of the same type from a source MAC address within a short time period. These attack packets consume many system resources of the AP, and therefore the AP cannot process packets from authorized STAs.

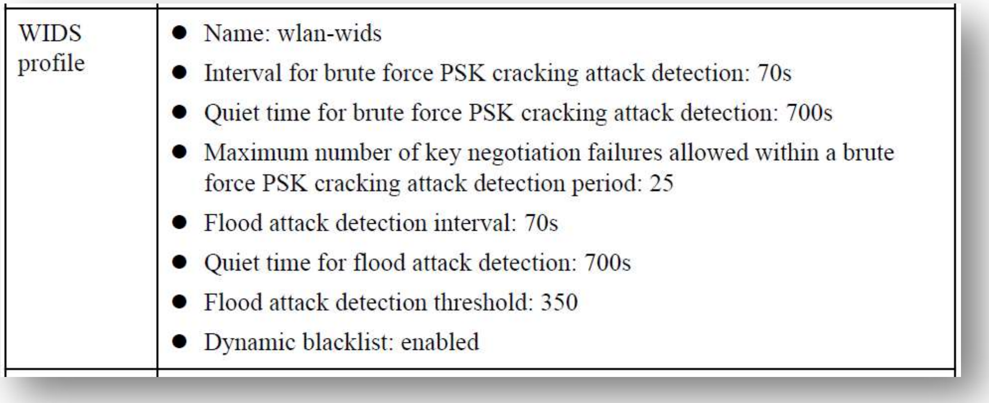
'690 PATENT CLAIM 33	INFRINGEMENT BY HUAWEI CORPORATION
	 Flood attack detection allows an AP to keep monitoring the traffic rate of each STA to defend against flood attacks. When the rate of traffic received from a STA exceeds the allowed threshold (for example, more than 100 packets per second), the AP considers that the STA will flood packets and reports an alarm to the AC. If the dynamic blacklist function is enabled, the detected attack STA will be added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the AP discards all the packets sent by this STA to protect the network against a flooding attack. An AP can detect flood attacks of the following types of frames: • Authentication Request • Deauthentication frame • Association Request • Disassociation frame • Probe Request • Action frame (extended management frame, which is used for spectrum management, QoS, and HT mode setting) • EAPOL Start frame • EAPOL-Logoff frame • PS-Poll frame (management frame sent by a STA when it recovers from the power-saving mode)

'690 PATENT CLAIM 33	**INFRINGEMENT BY HUAWEI CORPORATION**
	Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12-13. On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for collisions of packets of a predetermined type such as at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also monitor for collisions of packets of a predetermined type such as at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security."), 17.

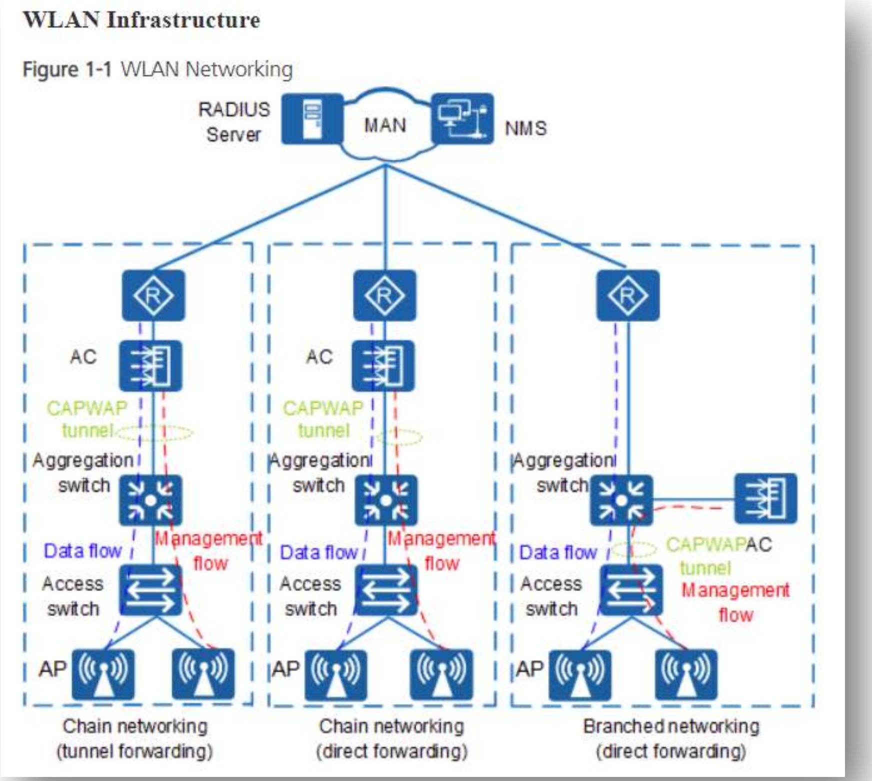
'690 PATENT CLAIM 34	**INFRINGEMENT BY HUAWEI CORPORATION**
34. The wireless network of claim 32 wherein the threshold number of collisions is greater than about three.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32. Further, the threshold number of collisions is greater than about three  By default, when the system receives 300 (x) packets of the same type within 60 (y)

'690 Patent Claim 34	**Infringement By Huawei Corporation**
	seconds (x and y are configurable), it considers that the packet sender initiates a flood attack. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12-13. In another configuration example provided in Huawei documentation, by default, the broadcast flood detection function is enabled, and the WIDS threshold may be configured to be 350 packets within 70 seconds: Step 7 Adjust WLAN high-density parameters. … # Enable the broadcast flood detection function and set a broadcast flood threshold. By default, the broadcast flood detection function is enabled. [AC-wlan-net-prof-wlan-net] undo anti-attack broadcast-flood disable [AC-wlan-net-prof-wlan-net] **quit** HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 79. 4.15.2 Example for Configuring Attack Detection

'690 PATENT CLAIM 34	INFRINGEMENT BY HUAWEI CORPORATION
	. . . **Figure 4-66** Networking for configuring attack detection  IP Network Router GE1/0/0 VLANIF101 Management VLAN: VLAN100 10.23.101.2/24 Service VLAN: VLAN101 GE0/0/3 GE0/0/1 GE0/0/1 GE0/0/2 SwitchB STA AP SwitchA GE0/0/2 GE0/0/1 AC VLANIF100 10.23.100.1/24

’690 PATENT CLAIM 34	INFRINGEMENT BY HUAWEI CORPORATION
	 WIDS profile ● Name: wlan-wids ● Interval for brute force PSK cracking attack detection: 70s ● Quiet time for brute force PSK cracking attack detection: 700s ● Maximum number of key negotiation failures allowed within a brute force PSK cracking attack detection period: 25 ● Flood attack detection interval: 70s ● Quiet time for flood attack detection: 700s ● Flood attack detection threshold: 350 ● Dynamic blacklist: enabled HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 693-695.

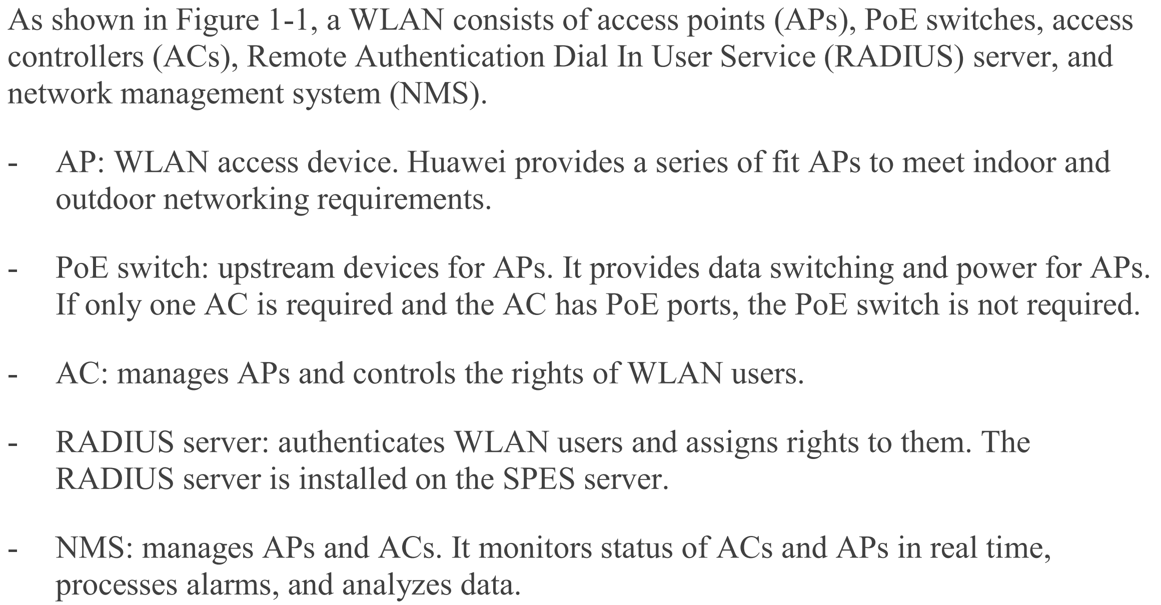
’690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
36. The wireless network of claim 32 wherein said plurality of stations transmit data via a medium access control (MAC) layer; wherein each station has a MAC address associated therewith to be transmitted with data	The Huawei ’690 Patent Accused Products infringe this claim. *See* Claim 32. The wireless network of claim 32 further contains functionality wherein said plurality of stations transmit data via a medium access control (MAC) layer; wherein each station has a MAC address associated therewith to be transmitted with data sent therefrom; One exemplary network configuration is shown:

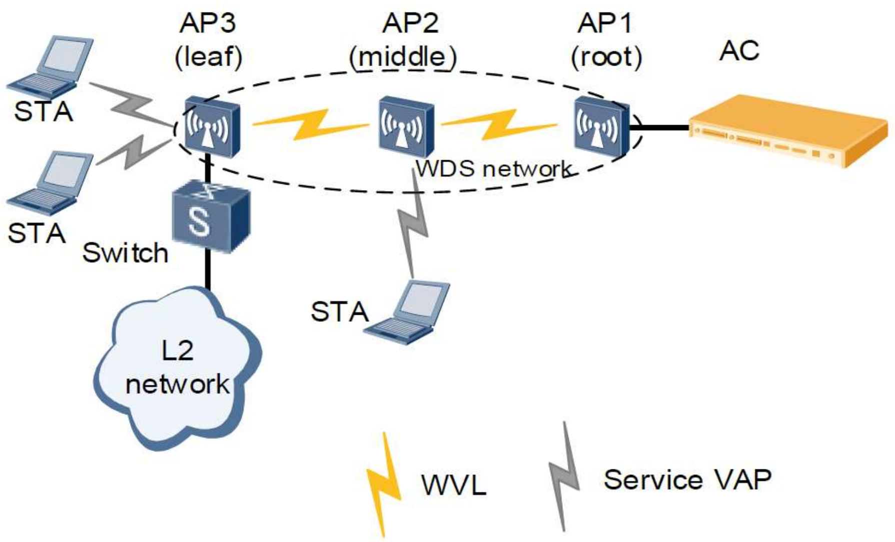
<table>
<tr><th>'690 PATENT
CLAIM 36</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td>sent therefrom; and wherein said policing station further detects intrusions into the wireless network by:</td><td>


WLAN Infrastructure

Figure 1-1 WLAN Networking

</td></tr>
</table>

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	 As shown in Figure 1-1, a WLAN consists of access points (APs), PoE switches, access controllers (ACs), Remote Authentication Dial In User Service (RADIUS) server, and network management system (NMS). - AP: WLAN access device. Huawei provides a series of fit APs to meet indoor and outdoor networking requirements. - PoE switch: upstream devices for APs. It provides data switching and power for APs. If only one AC is required and the AC has PoE ports, the PoE switch is not required. - AC: manages APs and controls the rights of WLAN users. - RADIUS server: authenticates WLAN users and assigns rights to them. The RADIUS server is installed on the SPES server. - NMS: manages APs and ACs. It monitors status of ACs and APs in real time, processes alarms, and analyzes data. HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 2. https://support.huawei.com/enterprise/en/doc/EDOC1000184389/1d542042/introduction-to-wlan In another configuration example, a WDS (Wireless Distribution System) may wirelessly connect two WLANs:

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 1-1 WDS network  AP3 (leaf) AP2 (middle) AP1 (root) AC STA STA Switch WDS network STA L2 network WVL Service VAP Huawei Technologies Co., Ltd. WLAN WDS Technology White Paper Issue 03 (2017-11-21) at 1-2.

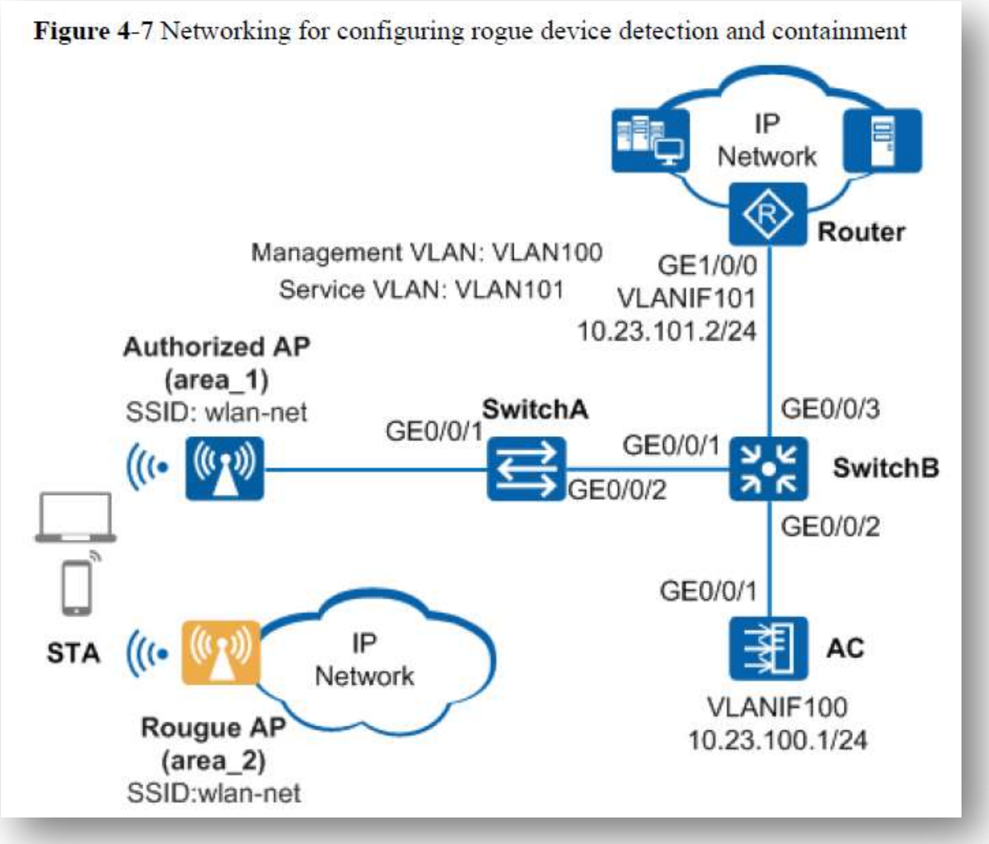
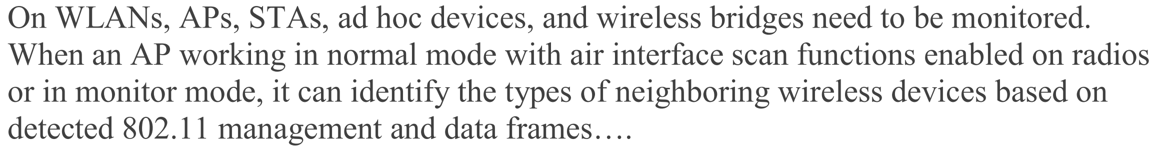
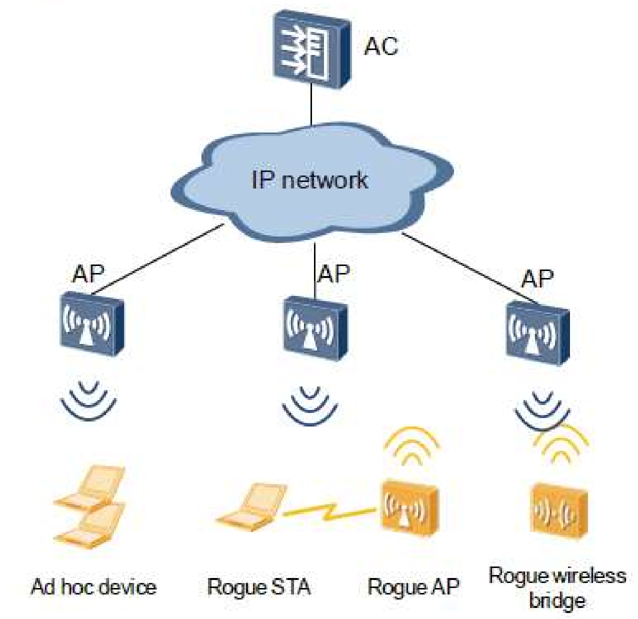
<table>
<tr><th>'690 PATENT
CLAIM 36</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>


Figure 4-7 Networking for configuring rogue device detection and containment

HUAWEI WLAN Typical Configuration Examples, Issue 01 (2017-12-29) at 123.
</td></tr>
</table>

'690 Patent Claim 36	**Infringement By Huawei Corporation**
	 On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames…. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4. For example, the network and network stations use the 802.11 standards format and transmit MAC address information in packets:

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	Figure 2-3 Rogue device detection and identification  AC IP network AP AP AP Ad hoc device Rogue STA Rogue AP Rogue wireless bridge The AP identifies the types of neighboring wireless devices based on detected 802.11 management and data frames.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION

The **Frame Control** field in the MAC header of a frame indicates the frame type. Figure 2-4 shows the subfields of the **Frame Control** field.

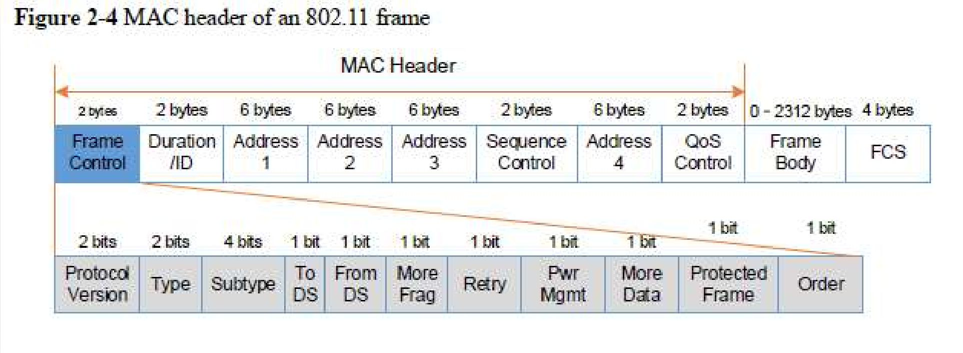


Figure 2-4 MAC header of an 802.11 frame

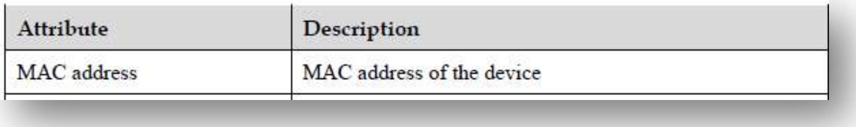
MAC Header

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	2 bytes	0 - 2312 bytes	4 bytes
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	Frame Body	FCS

2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	Protected Frame	Order

Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 5.

Each station has a MAC address associated therewith

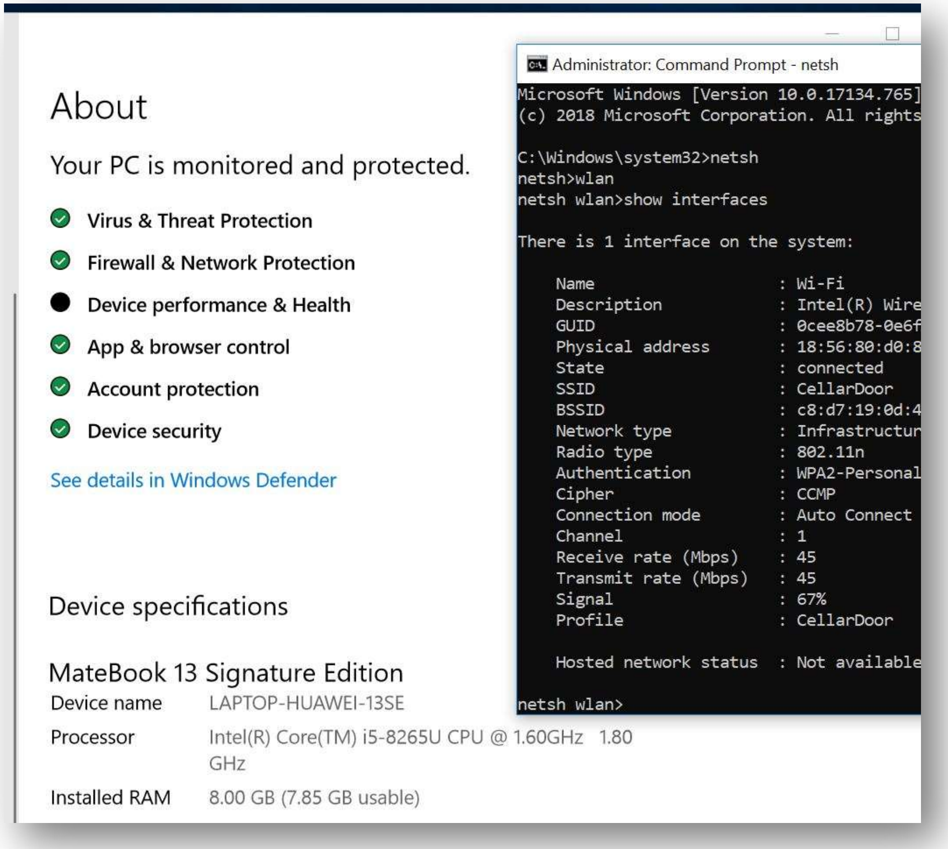


Attribute	Description
MAC address	MAC address of the device

Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 9.

MAC address - A link layer address or physical address. It is six bytes long.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at 253. On information and belief Huawei consumer devices, including laptops, phones and tablets also have a MAC address associated therewith. For example, Huawei laptops and tablets such as the Matebook 13 have an associated MAC "physical address":

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	

About

Your PC is monitored and protected.

- Virus & Threat Protection
- Firewall & Network Protection
- Device performance & Health
- App & browser control
- Account protection
- Device security

See details in Windows Defender

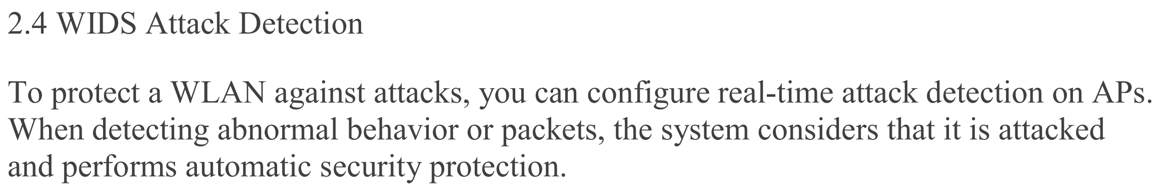
Device specifications

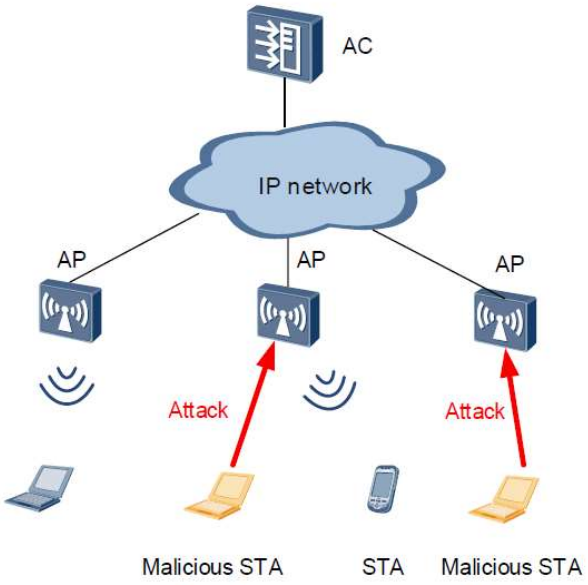
MateBook 13 Signature Edition

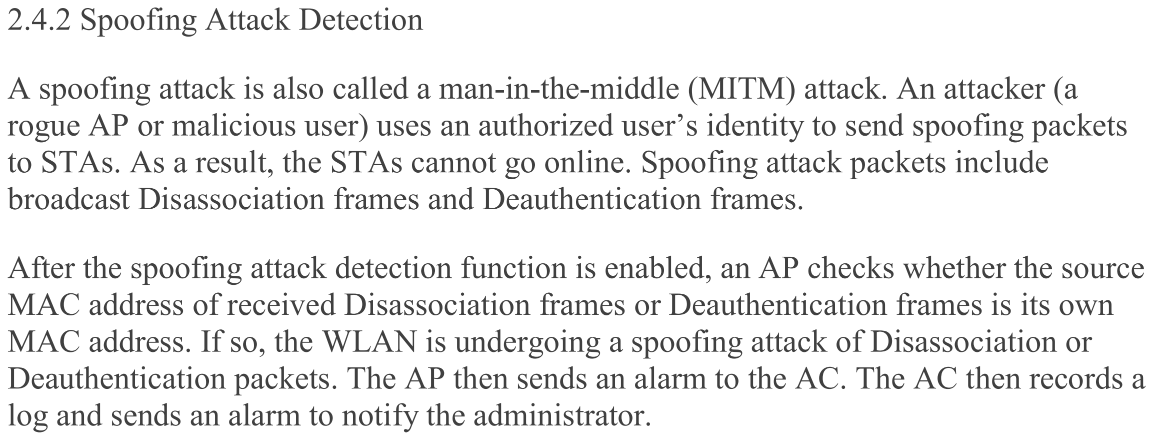
Device name	LAPTOP-HUAWEI-13SE
Processor	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
Installed RAM	8.00 GB (7.85 GB usable)

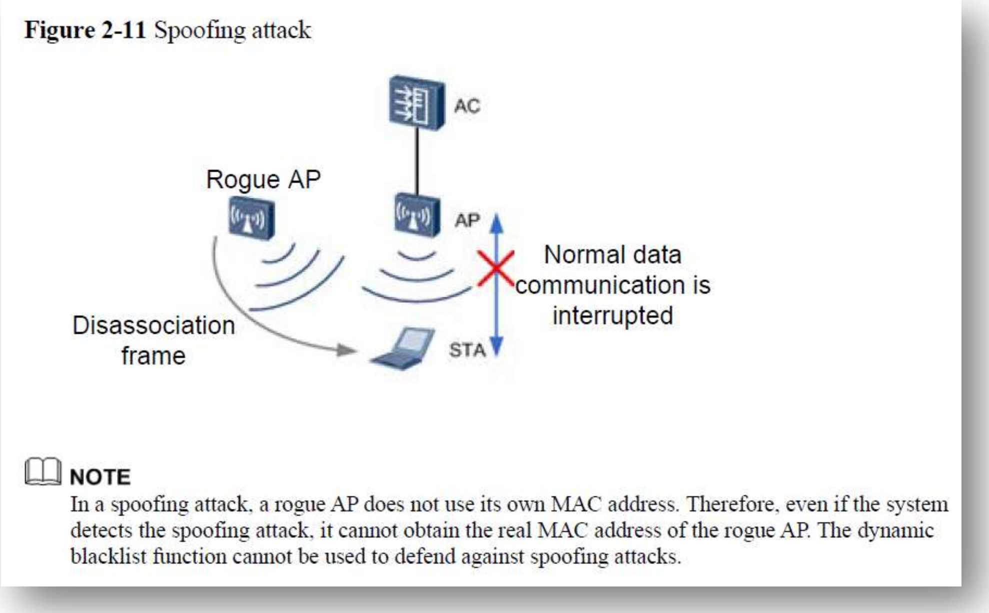
Administrator: Command Prompt - netsh

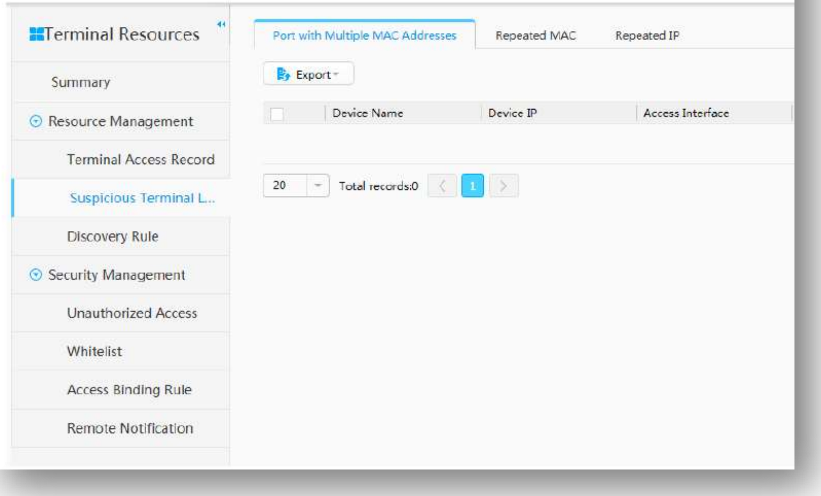
```
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights

C:\Windows\system32>netsh
netsh>wlan
netsh wlan>show interfaces

There is 1 interface on the system:

    Name                   : Wi-Fi
    Description            : Intel(R) Wire
    GUID                   : 0cee8b78-0e6f
    Physical address       : 18:56:80:d0:8
    State                  : connected
    SSID                   : CellarDoor
    BSSID                  : c8:d7:19:0d:4
    Network type           : Infrastructur
    Radio type             : 802.11n
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Connection mode        : Auto Connect
    Channel                : 1
    Receive rate (Mbps)    : 45
    Transmit rate (Mbps)   : 45
    Signal                 : 67%
    Profile                : CellarDoor

    Hosted network status  : Not available

netsh wlan>
```

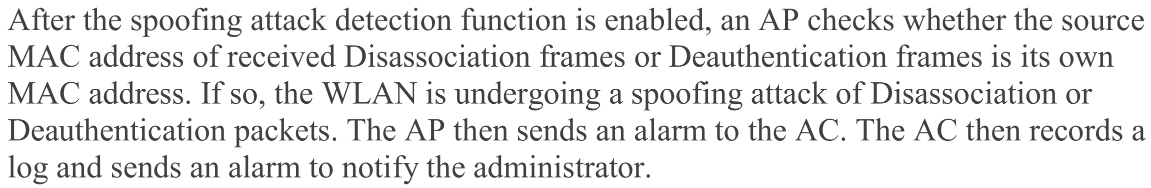
'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	The policing station further detects intrusions into the wireless network in the manner described below.
[a] monitoring transmissions among said plurality of stations to detect collisions of a same MAC address; and	The policing station can further detect intrusions into the wireless network by monitoring transmissions among said plurality of stations to detect collisions of a same MAC address. For example, the policing station is capable of detecting the use of a same MAC address:  2.4 WIDS Attack Detection To protect a WLAN against attacks, you can configure real-time attack detection on APs. When detecting abnormal behavior or packets, the system considers that it is attacked and performs automatic security protection.

'690 PATENT CLAIM 36	**INFRINGEMENT BY HUAWEI CORPORATION**
	Figure 2-9 WIDS attack detection scenario  AC IP network AP AP AP Attack Attack Malicious STA STA Malicious STA On the WLAN shown in the preceding figure, WIDS attack detection can be enabled on the AC when the WLAN access service is provided. The WIDS can detect 802.11 flood attacks, spoofing attacks, and weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 12.

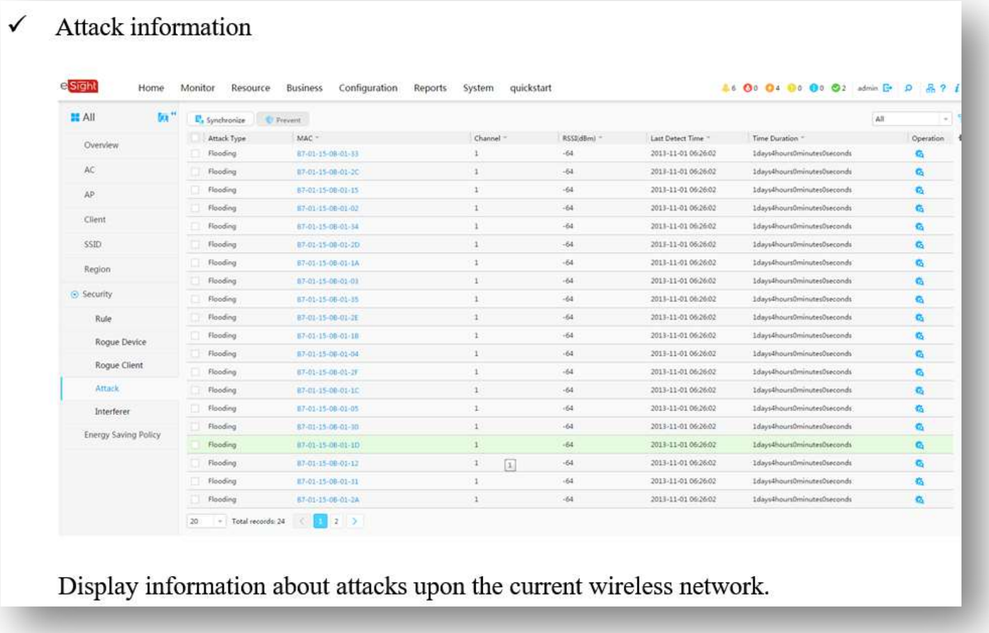
'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	 2.4.2 Spoofing Attack Detection A spoofing attack is also called a man-in-the-middle (MITM) attack. An attacker (a rogue AP or malicious user) uses an authorized user's identity to send spoofing packets to STAs. As a result, the STAs cannot go online. Spoofing attack packets include broadcast Disassociation frames and Deauthentication frames. After the spoofing attack detection function is enabled, an AP checks whether the source MAC address of received Disassociation frames or Deauthentication frames is its own MAC address. If so, the WLAN is undergoing a spoofing attack of Disassociation or Deauthentication packets. The AP then sends an alarm to the AC. The AC then records a log and sends an alarm to notify the administrator.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	 **Figure 2-11** Spoofing attack AC Rogue AP AP Normal data communication is interrupted Disassociation frame STA **NOTE** In a spoofing attack, a rogue AP does not use its own MAC address. Therefore, even if the system detects the spoofing attack, it cannot obtain the real MAC address of the rogue AP. The dynamic blacklist function cannot be used to defend against spoofing attacks. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 13-14. Further, on information and belief, when collisions of the same MAC addresses are detected, the AP and/or eSight identifies these as MAC address theft and reports them as suspicious terminals: Suspicious Terminal Report • Check invalid MAC addresses to detect unauthorized terminal access.

’690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	• Check duplicate MAC addresses to detect MAC address theft. • Check duplicate IP addresses to detect IP address theft. **Figure 2-37** Suspicious terminal  Terminal Resources Summary Resource Management Terminal Access Record Suspicious Terminal L... Discovery Rule Security Management Unauthorized Access Whitelist Access Binding Rule Remote Notification Port with Multiple MAC Addresses Repeated MAC Repeated IP Export Device Name Device IP Access Interface 20 Total records:0 1 *See e.g.,* eSight V300R007C00 Product Description, Issue 09 (2018-02-08) at 47. On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for collisions of a same MAC address, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei’s EMUI operating system, including its “Wi-Fi threat detection” functionality, also monitor for collisions of a same MAC address. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at

'690 Patent Claim 36	Infringement By Huawei Corporation
	https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").
[b] generating an intrusion alert based upon detecting a threshold number of collisions of a same MAC address.	The policing station, can further generate an intrusion alert based upon detecting a threshold number of collisions of a same MAC address.  After the spoofing attack detection function is enabled, an AP checks whether the source MAC address of received Disassociation frames or Deauthentication frames is its own MAC address. If so, the WLAN is undergoing a spoofing attack of Disassociation or Deauthentication packets. The AP then sends an alarm to the AC. The AC then records a log and sends an alarm to notify the administrator. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 13-14.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION



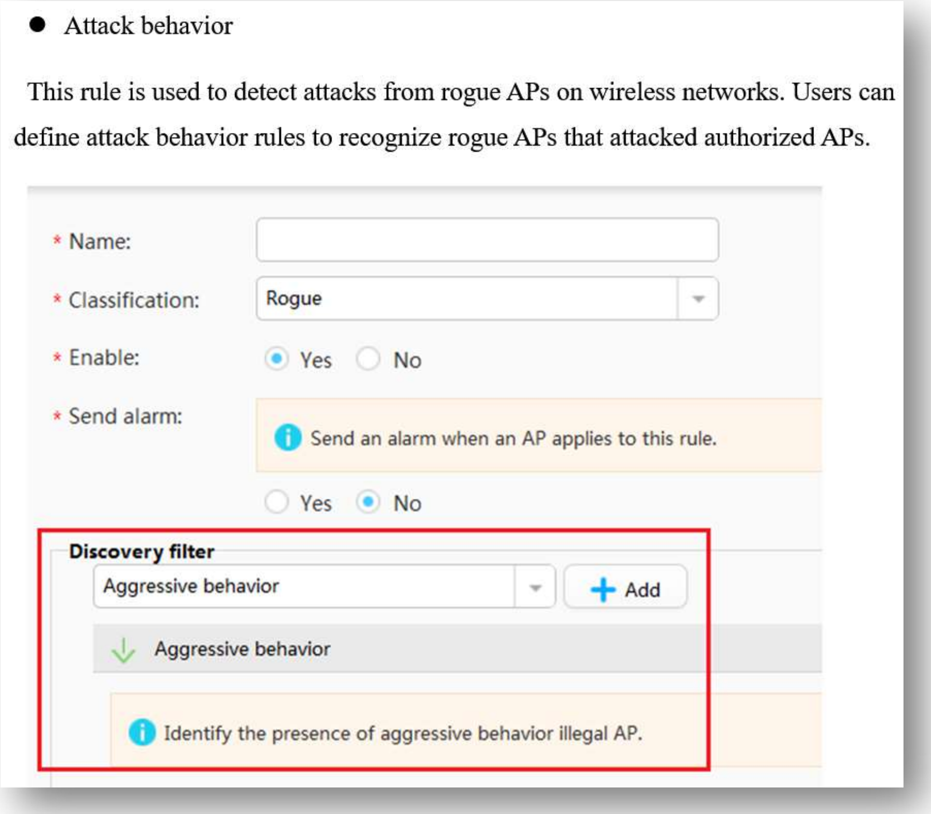
✓ Attack information

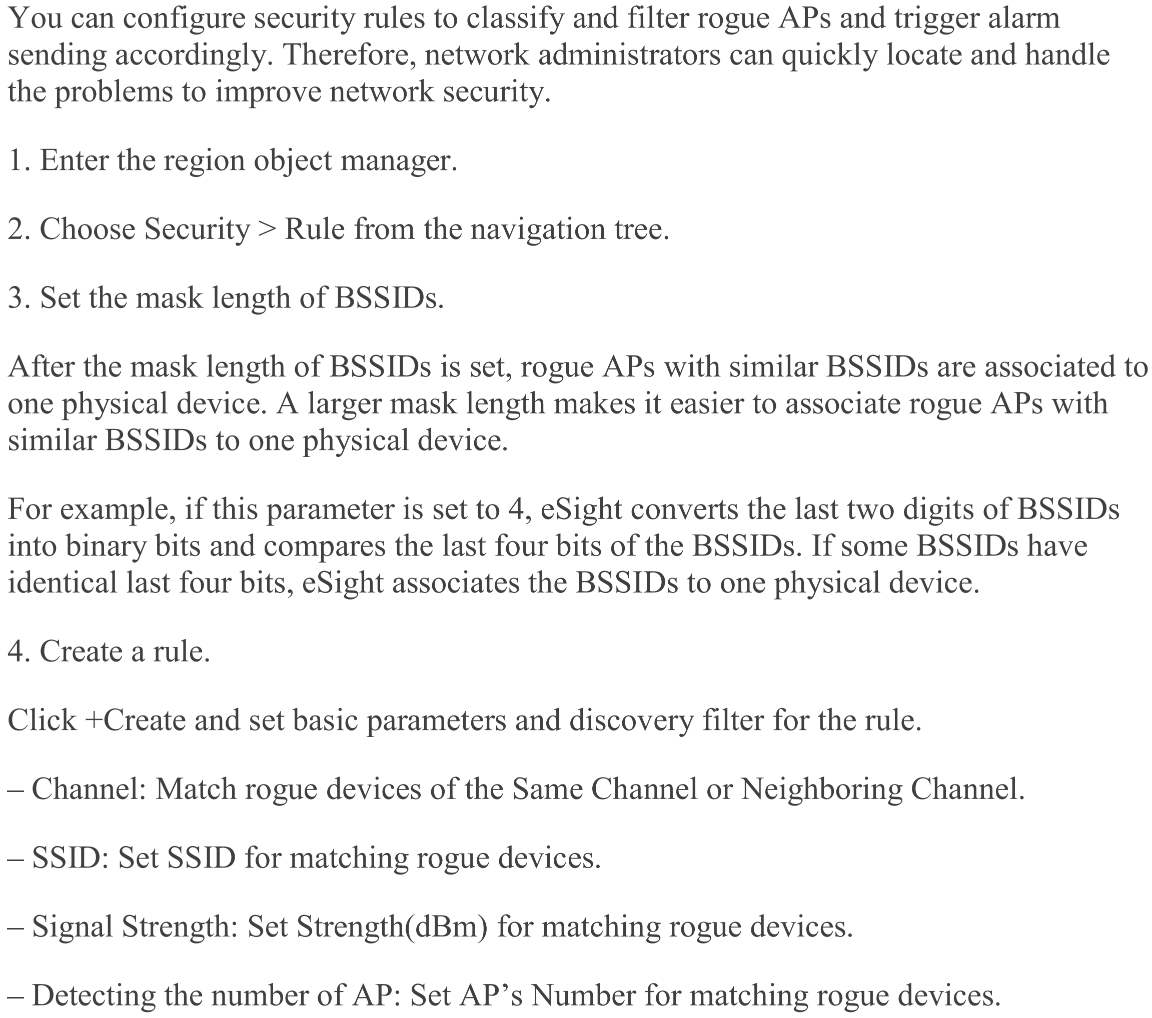
□	Attack Type	MAC	Channel	RSSI(dBm)	Last Detect Time	Time Duration	Operation
□	Flooding	B7-01-15-0B-01-33	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-2C	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-15	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-02	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-34	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-2D	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-1A	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-03	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-35	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-2E	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-1B	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-04	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-2F	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-1C	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-05	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-30	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-1D	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-12	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-31	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	
□	Flooding	B7-01-15-0B-01-2A	1	-64	2013-11-01 06:26:02	1days4hours0minutes0seconds	

20 Total records: 24 < 1 2 >

Display information about attacks upon the current wireless network.

HUAWEI eSight WLAN White Paper, Issue 01 (2017-03-20) at 11.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	 ● Attack behavior This rule is used to detect attacks from rogue APs on wireless networks. Users can define attack behavior rules to recognize rogue APs that attacked authorized APs. * Name: * Classification: Rogue * Enable: ● Yes ○ No * Send alarm: Send an alarm when an AP applies to this rule. ○ Yes ● No Discovery filter Aggressive behavior Aggressive behavior Identify the presence of aggressive behavior illegal AP. HUAWEI eSight WLAN White Paper, Issue 01 (2017-03-20) at 14.

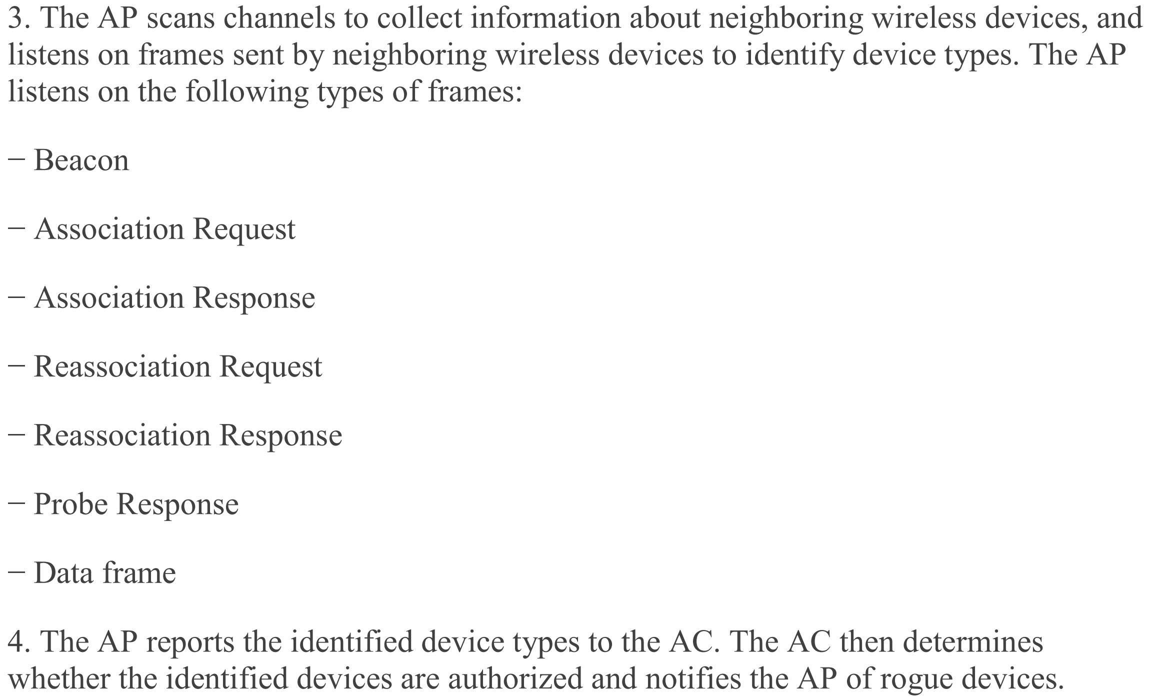
'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	 You can configure security rules to classify and filter rogue APs and trigger alarm sending accordingly. Therefore, network administrators can quickly locate and handle the problems to improve network security. 1. Enter the region object manager. 2. Choose Security > Rule from the navigation tree. 3. Set the mask length of BSSIDs. After the mask length of BSSIDs is set, rogue APs with similar BSSIDs are associated to one physical device. A larger mask length makes it easier to associate rogue APs with similar BSSIDs to one physical device. For example, if this parameter is set to 4, eSight converts the last two digits of BSSIDs into binary bits and compares the last four bits of the BSSIDs. If some BSSIDs have identical last four bits, eSight associates the BSSIDs to one physical device. 4. Create a rule. Click +Create and set basic parameters and discovery filter for the rule. – Channel: Match rogue devices of the Same Channel or Neighboring Channel. – SSID: Set SSID for matching rogue devices. – Signal Strength: Set Strength(dBm) for matching rogue devices. – Detecting the number of AP: Set AP's Number for matching rogue devices.

'690 PATENT CLAIM 36	INFRINGEMENT BY HUAWEI CORPORATION
	– Aggressive behavior: Specify this parameter for identifying rogue APs that make attacks. – Valid users association: Identify users that have connected to rogue APs. eSight Operation Guide, Issue 08 (2018-08-28) at 1357. On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on detecting a threshold number of collisions of a same MAC address, including when configured as a mobile hotspot. Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also generate an intrusion alert based on detecting a threshold number of collisions of a same MAC address. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

'690 PATENT CLAIM 37	INFRINGEMENT BY HUAWEI CORPORATION
37. The wireless network of claim 32 wherein the	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32.

'690 Patent Claim 37	**Infringement By Huawei Corporation**
threshold number of collisions is greater than about three.	Further, the threshold number of collisions is greater than about three. *See* Claim 34.

'690 Patent Claim 38	**Infringement By Huawei Corporation**
38. The wireless network of claim 32 wherein said policing station further transmits an intrusion alert to at least one of said plurality of stations.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32. Further, said policing station further transmits an intrusion alert to at least one of said plurality of stations. For example, the monitor AP generates and transmits intrusion alert information to the AC, and the AC reports intrusion alert information: On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows: 1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios. 2. The AC delivers the configuration to the AP.

'690 PATENT CLAIM 38	INFRINGEMENT BY HUAWEI CORPORATION
	 3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames: – Beacon – Association Request – Association Response – Reassociation Request – Reassociation Response – Probe Response – Data frame 4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices. Huawei Technologies Co., Ltd. *WLAN WIDS & WIPS Technology White Paper*; Issue 2.0 (2017-07-05) at 4.

'690 PATENT CLAIM 39	**INFRINGEMENT BY HUAWEI CORPORATION**
39. The wireless network of claim 32 wherein said policing station comprises at least one of a base station and a wireless station.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32. Further, the policing station in the wireless network of claim 32 comprises at least one of a base station and a wireless station. For example, the policing station may be a Monitor AP. *See* claim 32[b] above.

'690 PATENT CLAIM 40	**INFRINGEMENT BY HUAWEI CORPORATION**
40. A wireless local or metropolitan area network comprising:	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 32 [preamble].
[a] a plurality of stations for transmitting data via a medium access control (MAC) layer, each station having a MAC address associated therewith to be transmitted with data sent therefrom; and	The Huawei '690 Patent Accused Products comprise a plurality of stations for transmitting data via a medium access control (MAC) layer, each station having a MAC address associated therewith to be transmitted with data sent therefrom. *See* Claim 36.

'690 Patent Claim 40	**Infringement By Huawei Corporation**
[b] a policing station for detecting intrusions into the wireless network by	The Huawei '690 Patent Accused Products comprise a policing station for detecting intrusions into the wireless network *See* Claim 32[b]
[c] monitoring transmissions among said plurality of stations to detect collisions of a same MAC address; and	The Huawei '690 Patent Accused Products are capable of monitoring transmissions among said plurality of stations to detect collisions of a same MAC address. *See* Claim 36[a].
[d] generating an intrusion alert based upon detecting a threshold number of collisions of a same MAC address.	The Huawei '690 Patent Accused Products are capable of generating an intrusion alert based upon detecting a threshold number of collisions of a same MAC address. *See* Claim 36[b].

'690 Patent Claim 41	**Infringement By Huawei Corporation**
41. The wireless network of claim 40 wherein the threshold number of collisions is greater than about three.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 40 Further, the threshold number of collisions is greater than about three. *See* Claim 34.

'690 PATENT CLAIM 42	INFRINGEMENT BY HUAWEI CORPORATION
42. The wireless network of claim 40 wherein said policing station further transmits an intrusion alert to at least one of said plurality of stations.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 40 Further, said policing station further transmits an intrusion alert to at least one of said plurality of stations. *See* Claim 38.

'690 PATENT CLAIM 43	INFRINGEMENT BY HUAWEI CORPORATION
43. The wireless network of claim 40 wherein said policing station comprises at least one of a base station and a wireless station.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 40. Further, said policing station comprises at least one of a base station and a wireless station. *See* Claim 39.

'690 PATENT CLAIM 71	INFRINGEMENT BY HUAWEI CORPORATION
71. An intrusion detection method for a wireless local or metropolitan area network comprising a plurality of	The Huawei '690 Patent Accused Products infringe this claim. The Huawei '690 Patent Accused Products use an intrusion detection method for a wireless local or metropolitan comprising a plurality of stations. *See* Claims 32[preamble], 32[a].

'690 PATENT CLAIM 71	**INFRINGEMENT BY HUAWEI CORPORATION**
stations, the method comprising:	
[a] transmitting data in packets between the plurality of stations, each packet having a packet type associated therewith;	The method of the Huawei '690 Patent Accused Products transmits data in packets between the plurality of stations, each packet having a packet type associated therewith. *See* Claim 32[a].
[b] monitoring transmissions among the plurality of stations to detect collisions of packets having a predetermined packet type; and	The method of the Huawei '690 Patent Accused Products monitors transmissions among the plurality of stations to detect collisions of packets having a predetermined packet type. *See* Claim 32 [c].
[c] generating an intrusion alert based upon detecting a threshold number of collisions of packets having the predetermined packet type.	The method of the Huawei '690 Patent Accused Products generates an intrusion alert based upon detecting a threshold number of collisions of packets having the predetermined packet type. *See* Claim 32 [d].

'690 PATENT CLAIM 72	INFRINGEMENT BY HUAWEI CORPORATION
72. The method of claim 71 wherein the predetermined packet type comprises at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 71. Further, the predetermined packet type comprises at least one of authentication packets, association packets, beacon packets, request to send (RTS) packets, and clear to send (CTS) packets. *See* Claim 33.

'690 PATENT CLAIM 73	INFRINGEMENT BY HUAWEI CORPORATION
73. The method of claim 71 wherein the threshold number of collisions is greater than about three.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 71. Further, the threshold number of collisions is greater than about three. *See* Claim 34.

'690 PATENT CLAIM 75	INFRINGEMENT BY HUAWEI CORPORATION
75. The method of claim 71 wherein the plurality of stations transmit data packets via a medium access control (MAC) layer, and wherein	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 71.

'690 PATENT CLAIM 75	**INFRINGEMENT BY HUAWEI CORPORATION**
each station has a MAC address associated therewith to be transmitted with data packets sent therefrom; and further comprising:	Further, the plurality of stations transmit data packets via a medium access control (MAC) layer, and wherein each station has a MAC address associated therewith to be transmitted with data packets sent therefrom. *See* Claim 36.
[a] monitoring transmissions among the plurality of stations to detect collisions of a same MAC address; and	The Huawei '690 Patent Accused Products monitor transmissions among the plurality of stations to detect collisions of a same MAC address *See* Claim 36[a]
[b] generating an intrusion alert based upon detecting a threshold number of collisions of a same MAC address.	The Huawei '690 Patent Accused Products generate an intrusion alert based upon detecting a threshold number of collisions of a same MAC address *See* Claim 36[b]

'690 PATENT CLAIM 76	**INFRINGEMENT BY HUAWEI CORPORATION**
76. The method of claim 75 wherein the threshold number of collisions is greater than about three.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 75. Further, the threshold number of collisions is greater than about three. *See* Claim 34.

'690 Patent Claim 77	**Infringement By Huawei Corporation**
77. The method of claim 71 further comprising transmitting the intrusion alert to at least one of the plurality of stations.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 71. Further, the method comprises transmitting the intrusion alert to at least one of the plurality of stations *See* Claim 38.

'690 Patent Claim 78	**Infringement By Huawei Corporation**
78. An intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations, the method comprising:	The Huawei '690 Patent Accused Products infringe this claim. The Huawei '690 Patent Accused Products use an intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations *See* Claim 32 [preamble], 32[a].
[a] transmitting data via a medium access control (MAC) layer between the plurality of stations, each station having a MAC address associated therewith to be transmitted with data sent therefrom;	The method used in the Huawei '690 Patent Accused Products transmits data via a medium access control (MAC) layer between the plurality of stations, each station having a MAC address associated therewith to be transmitted with data sent therefrom *See* Claims 36 [a]; 40 [a]

'690 PATENT CLAIM 78	INFRINGEMENT BY HUAWEI CORPORATION
[b] monitoring transmissions among the plurality of stations to detect collisions of a same MAC address; and	The method used in the Huawei '690 Patent Accused Products monitors transmissions among the plurality of stations to detect collisions of a same MAC address *See* Claims 36 [a]; 40[c]
[c] generating an intrusion alert based upon detecting a threshold number of collisions of a same MAC address.	The method used in the Huawei '690 Patent Accused Products generates an intrusion alert based upon detecting a threshold number of collisions of a same MAC address. *See* Claims 36 [b]; 40[d]

'690 PATENT CLAIM 79	INFRINGEMENT BY HUAWEI CORPORATION
79. The method of claim 78 wherein the threshold number of collisions of a same MAC address is greater than about three.	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 78. Further, the threshold number of collisions of a same MAC address is greater than about three. *See* Claim 34

'690 PATENT CLAIM 80	INFRINGEMENT BY HUAWEI CORPORATION
80. The method of claim 78 further comprising	The Huawei '690 Patent Accused Products infringe this claim. *See* Claim 78.

transmitting the intrusion alert to at least one of the plurality of stations.	The Instrumentalities further are capable of transmitting the intrusion alert to at least one of the plurality of stations. *See* claim 38.